This project has received funding from the European Union's Horizon 2020 Programme

RESEARCH PROJECT EASA.2020.C43

QUICK RECOVERY OF FLIGHT RECORDER DATA (wireless transmission)

Report D7

Scenario-based study of legal aspects

An Agency of the European Union

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

DELIVERABLE NUMBER AND TITLE:	QR-FRD D7 Scenario-based study of legal aspects
CONTRACT NUMBER:	EASA.2020.C43
CONTRACTOR / AUTHOR:	Collins Aerospace / Safran E&D / B. de Courville Consulting
IPR OWNER:	European Union Aviation Safety Agency
DISTRIBUTION:	Public

APPROVED BY:	MAIN AUTHORS	REVIEWERS	MANAGING DEPARTMENT
	Bertrand de Courville Simon Foreman Aurélie Girault	Carla Ramos (EASA) Guillaume Aigoin (EASA)	

DATE: 23 August 2022

REPORT D7

Scenario-based study of legal aspects

Submitted to:

EASA

European Union Aviation Safety Agency

Cologne, Germany

Document Information	
Customer reference	EASA.2020.HVP.06
Project Title	Quick Recovery of Flight Recorder Data
Contract number	EASA.2020.C43
Consortium	Collins Aerospace / Safran E&D / B. de Courville Consulting
Task Number	07
Task Title	Scenario-based study of legal aspects
Deliverable Name	D7 - Scenario-based study of legal aspects
Edition	01
Milestone Due Date	August 23rd, 2022
Dissemination Level	Public

Table of content

1 Introduction

1.1 QR-FRD Study Presentation

"The overarching objective of the Quick Recovery of Flight Recorder Data (QR-FRD) study is to identify and assess technical solutions for the automatic wireless data transmission to quickly recover flight recorder data after an accident in a remote land area or an oceanic area for the purpose of faster understanding of the causal and contributory factors of an accident" (EASA QR-FRD CFT).

The overall objectives of the project are to identify and to assess a series of candidate solutions for the wireless transmission of flight recorder data from commercial air transport aircraft in case of an accident (or a serious incident) in a remote land area or an oceanic area while considering thoroughly the challenges, constraints and limitations of each technical solution and the challenging conditions of an accident (or a serious incident).

The evaluation of the candidate solutions will address the technical feasibility and maturity, the performance, the related constraints as well as the cost indicators in comparison to current flight data recorder installations.

The aircraft considered for the study are modern commercial air transport aircraft with a maximum take-off mass of over 27 tons and authorized to carry more than nineteen passengers, equipped with redundant combined flight data recorder (FDR) -cockpit voice recorder (CVR) capable of recording flight data, flight crew and cockpit area microphone audio, data link messages as well as, depending on the type certificate, flight crew – machine interface recordings (ICAO Annex 6 Part I, Section 6.3 [Ref 6]), and mandated to have a Flight Recorder Data Recovery (FRDR) means on-board.

A further investigation of the performance levels achievable will be carried out by developing several simulation exercises for two of the candidate solutions, applying representative operational conditions for aircraft accidents (and serious incidents) and aiming at analyzing the options for recovering the most useful data. In addition, the legal implications associated to the wireless transmission of flight recorder data, considering the existing data protection frameworks and the related ICAO Annex 13 [Ref 8] provisions will be investigated.

The results of the feasibility project, together with the practical recommendations for the implementation of the candidate solutions, will be presented to a group of stakeholders involved in accident investigations and consolidated with the feedback received.

The activities undertaken within the QR-FRD study, and their respective documented outcomes are the following:

1. Task 1 - Accident conditions relevant for wireless flight recorder data transmission:
    - **Objective**: Identify and describe the technical and environmental factors which might affect the aircraft, its engines and its systems during the accident flight, and which need to be taken into account for maximizing the chances of successful wireless transmission of flight recorder data.
      Outcome: A report (D1) of accident conditions which might affect the successful wireless transmission of flight recorder data (e.g., loss of power or equipment, excessive roll or pitch angles, in-flight fire, ditching …), and explaining the impact of such factors. that describes the considered factors.

2. Task 2 - Overview of technical solutions for automatic wireless transmission of flight recorder data:
    - **Objective**: perform a screening of possible technical solutions for automatic wireless transmission of flight recorder data (flight data, audio and flight-crew interface recordings, data link messages…) in case of an accident (or serious incident) in a remote land area or an oceanic area.
    - **Outcome**: A solution overview report (D2) identifying the necessary technologies and capabilities of the communication infrastructure, as well as aspects not yet mature, and discussing the potential effects of factors listed in D1 on the presented solutions. In addition, D2 will recommend the 2 most relevant technical solutions for further investigation to be performed under Task 3.
3. Task 3 - Technical investigation of two technical solutions for automatic wireless transmission of flight recorder data:
    - **Objective**: perform a technical investigation of the two most relevant technical solutions as identified in Task 2 and assess their performances for the automatic and wireless transmission of the data required to be recorded and retained by crash-protected flight recorders.
    - **Outcome**: A study report (D3) presenting technical solutions and detailing the two selected technical solutions (concept of operation, data transmission trigger logic (e.g. continuous or triggered), airborne functions and equipment, performance, communication infrastructure…).
4. Task 4 – Assess challenges and limitations of two technical solutions:
    - **Objective**: Assess the challenges and limitations of both technical solutions presented in Task 3 and comparison of their expected performance.
    - **Outcome**: An evaluation report (D4) of challenges and limitations addressing main technological enablers and their respective levels of maturity, reliability of main functions, impacts on flight crew procedures, ground handling and maintenance, as well as airline operations…
5. Task 5 – First consultation of the stakeholder's group:
    - **Objective**: Obtain the feedback of a group of stakeholders (accident investigation authorities, aviation regulators, operators of large commercial aircraft, associations of commercial pilots) on works performed under Tasks 1 to 4, with a view to incorporate this feedback into the analyses and assessments and to update the corresponding reports.
    - **Outcome**: A stakeholder feedback report (D5) containing the composition of the group of stakeholders, comments and questions raised by the stakeholders and replies as well as changes made to the different reports (D1 to D4).
6. Task 6 – Simulation of technical solutions:
    - **Objective**: Prepare an experimental set-up for the performance assessment of the two solutions investigated in Task 3, in particular for the comparison of the respective transmitted dataset (volume, accuracy, completeness, consistency) including reliability and robustness to factors identified in Task 1.
    - **Outcome**: A simulation report (D6) containing the detailed description of the performed simulations, as well as graphics showing the variation in performance when parameters (pitch and roll angles/rates, altitude, location of the aircraft…) are varied.

7. Task 7 - Scenario-based study of legal aspects:
    - **Objective**: Assess the legal aspects of data transmission over assets located on the territories of several countries or in space, in order to identify possible inconsistencies with ICAO Annex 13, legal uncertainties and risks for the protection of flight recorder data.
    - **Outcome**: A legal study report (D7) describing the legal framework applicable to the various assets of the communication infrastructure by which data will be transmitted or processed or recorded, scenarios of accidents in various places and with various setups, the potential issues for the protection and the transmission of data to the competent safety investigation authority, as well as proposals to ensure that the transmission service provider and the recipient of the flight recorder data are legally responsible for the preservation and the protection of transmitted flight recorder data.

8. Task 8 – Second consultation of the stakeholder's group and additional simulation work:
    - **Objective**: Obtain the assessment of a group of stakeholders on the report resulting from Tasks 6 and 7, with a view to incorporate this feedback, to run where necessary complementary simulations and to update the simulation report.
    - **Outcome**: A stakeholder feedback report (D8) containing the composition of the group of stakeholders, comments and questions raised by the stakeholders and replies as well as changes made to the different reports (D6 and D7), and possibly simulations and code.
9. Task 9 – Conclusions and way forward:
    - **Objective**: Conclude on the concept of automatic wireless transmission of flight recorder data in case of an accident and propose a way forward.
    - **Outcome**: A final report (D9) containing a general reflection on the works performed during the project, the feedback and recommendations received during the stakeholder meetings, the aspects of the concept of automatic wireless transmission of flight recorder data remaining to be explored or showing very challenging issues, a proposed approach for the development of compliance means and material in order to facilitate the performance demonstration to competent authorities, as well as practical recommendations to progress the maturity of this concept and prepare their implementation.

The figure below depicts the overall approach taken for the QR-FRD study and the relationship between the different deliverables.

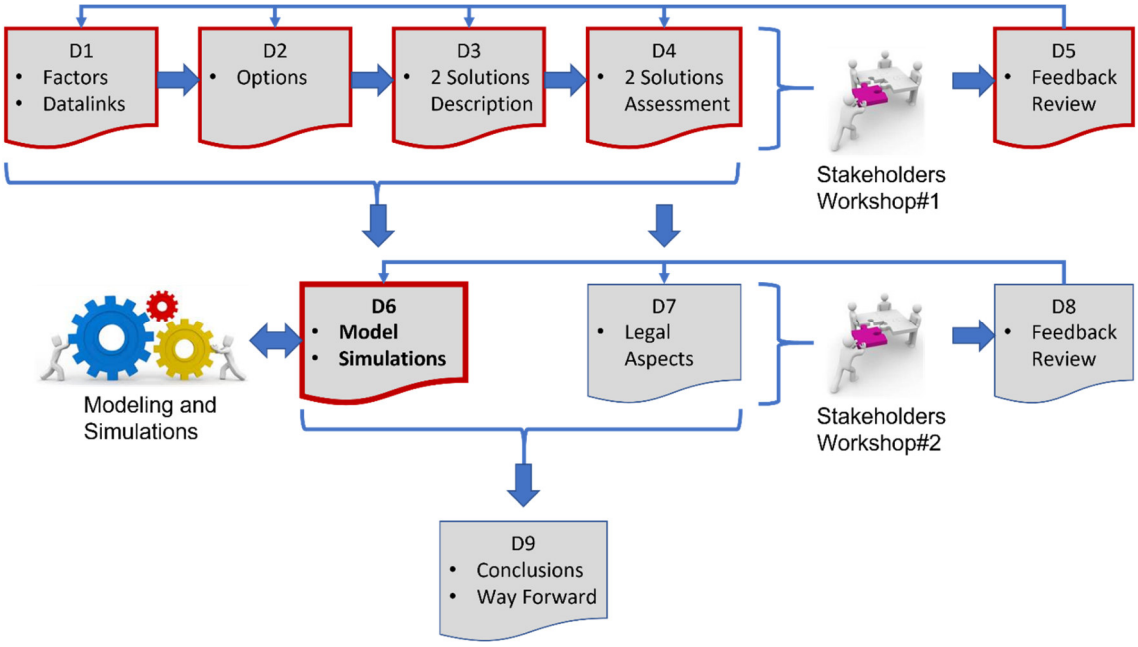


Figure 1: QR-FRD Study Approach and Deliverables Relationship

1.2 Scope of this report

This report summarizes analysis and findings from task 7 “Scenario-based study of legal aspects” of the solutions presented in the present Quick Recovery of Flight Recorder Data (QR-FRD) study.

It aims at assessing the legal aspects of data transmission over assets located on the territories of several countries or in space, to identify possible inconsistencies with ICAO Annex 13 [Ref 8][Ref 8] , legal uncertainties, and risks for the protection of flight recorder data.

Even though serious incidents are not formally in the scope of the study (see the study’s call for tender EASA.2020.HVP.06) the QR-FRD, as it is thought to facilitate data access, could be used by the AIA’s when investigating on serious incidents. This pragmatic observation justifies including serious incident in the scope of this report. However, such use may require rules to be set out to limit AIA’s permanent access and should be assessed in terms of costs.

1.3 Background

The Quick Recovery of Flight Recorder Data (QR-FRD) study aims at defining and assessing solutions for wireless transmission of flight recorder data. This is one of the two approaches investigated so far to timely recover flight recorder data for investigations after an accident, the other being the use of automatic deployable flight recorders (ADFR).

1.4 Organization of the document

This document develops the issues identified during the Task 4 “Assess challenges and limitations of the two solutions” [Ref 4] of the QR-FRD study, and is organized as follows:

Chapter 1, “INTRODUCTION”, (the present chapter), primarily provides background information on the initiation of QR-FRD studies and defines the scope of the present document.

Chapter 2, “REFERENCE DOCUMENTS”, provides the list of reference documents used for the drafting of the present document.

Chapter 3, “DEFINITIONS AND ACRONYMS”, provides definitions of terms and acronyms used in the present document.

Chapter 4, “PRELIMINARY CHAPTER” presents the general legal framework and main useful legal concepts and describes accident scenarios.

Chapter 5, “LEGAL FRAMEWORK APPLICABLE TO BOTH TECHNICAL SOLUTIONS” analyses the legal framework and issues for each functional blocks (FBs).

2 Reference documents

[Ref 1] QR-FRD Study D1: “Accident conditions relevant for wireless flight recorder data transmission”, Ed 02, April 2022
[Ref 2] QR-FRD Study D2: “Overview of Technical Solutions for Automatic Wireless Transmission”, Ed 01, April 2022
[Ref 3] QR-FRD Study D3: “Technical investigation of the two solutions”, Ed 01, April 2022
[Ref 4] QR-FRD Study D4: “Assess challenges and limitations of the two solutions”, Ed 01, April 2022
[Ref 5] QR-FRD Study D6: “Simulation of Technical Solutions”
[Ref 6] ICAO Annex 6 “Operation of Aircraft” 11th Edition, July 2018
[Ref 7] ICAO Annex 10 “Aeronautical Telecommunications”, 7th Edition, July 2018
[Ref 8] ICAO Annex 13 “Aircraft Accident and Incident Investigation”, 12th Edition, July 2020
[Ref 9] ICAO Annex 19 “Safety Management”, 2nd Edition, July 2016
[Ref 10] ICAO 9718 “Handbook on Radio Frequency Spectrum Requirements for Civil Aviation - Volume II — Frequency assignment planning criteria for aeronautical radio communication and navigation systems”, 2nd Edition, 2022
[Ref 11] ICAO 9756 “Manual of Aircraft Accident and Incident Investigation”, 1st Edition, 2016
[Ref 12] ICAO 9859 “Safety Management Manual”, 4th Edition, 2018
[Ref 13] ICAO 10053 “Manual on the Protection of Safety Information”, 1st Edition, 2019
[Ref 14]
[Ref 15] ICAO 10054 “Manual on Location of Aircraft in Distress and Flight Recorder Data Recovery”, 1st Edition, 2019
[Ref 16] ICAO CAST Common Taxonomy Team Document
[Ref 17] ICAO "Aviation Cybersecurity Strategy", October 2019
[Ref 18] ICAO “Cybersecurity Action Plan”, 2nd Edition, January 2022
[Ref 19] Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC
[Ref 20] Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC
[Ref 21] Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to
[Ref 22] Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007

[Ref 23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[Ref 24] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91
[Ref 25] Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[Ref 26] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
[Ref 27] Directive 2016/1148 concerning measures for a high-level security of network and information systems across the Union Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services
[Ref 28] Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
[Ref 29] Judgment of the Court (Grand Chamber) of 16 July 2020, “Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems”, No. C-311/18, ECLI:EU:C:2020:559
[Ref 30] EDBP, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Adopted on 25 May 2018
[Ref 31] EDPB, Recommendations 01/2020 on measures to complement transfer instruments to ensure compliance with the EU level of personal data protection of 18 June 2021
[Ref 32] ISO/IEC 27001:2017 — Information security management — Information technology
[Ref 33] ISO/IEC 27002 :2013 — Information technology — Security techniques — Code of practice for information security controls.
[Ref 34] ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.
[Ref 35] ISO/IEC 27018 :2019 — Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
[Ref 36] ISO/IEC 27040:2015 – Information technology – Security techniques – Storage security.
[Ref 37] ISO/IEC 22237-x — Information technology — Data centre facilities and infrastructures.
[Ref 38] EN 50600-x-y — Information technology — Data centre facilities and infrastructures
[Ref 39] EUROCAE ED-237 - MASPS for Criteria to detect In-Flight Aircraft Distress Events to trigger Transmission of Flight Information

3 Definitions and acronyms

3.1 Definitions

This section aims to clarify the definitions of important notions and main distinctions used in the report

Accident (ICAO Annex 13 [Ref 8] definition). ***"****An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which: a) a person is fatally or seriously injured (…) or b) the aircraft sustains damage or structural failure (…) or c) the aircraft is missing or is completely inaccessible"*.

Blockchain: the blockchain is a series of records (called block) linked in a secure way by a cryptographic hash. Each block contains the cryptographic hash of the previous block, the timestamp and data. The inviolability of the information is guaranteed by the fact that the inscription of a new block requires the agreement of the majority of the chain users.

Conflict of interest (COI): a situation of interference between a public interest and private or public interests that is likely to influence or appear to influence the independent, impartial, and objective exercise of a function.

For the study, the implementation of the QR-FRD is considered as being in the public interest as it improves aviation safety.

Data controller: in EU Regulation n°2016/679 [Ref 23] (hereafter, the "GDPR"), relating to personal data, the data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data[1]. This study has adopted the same definition for all data, personal or not.

Data processing: in EU Regulation n°2016/679 [Ref 23] (hereafter, the "GDPR") regarding personal data, "*processing means any operation or set of operations which is performed on (personal) data or on sets of (personal) data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"[2]. This study has adopted the same definition for all data, personal or not.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Flight recorder (Ref. definition QR-FRD Study report D6 [Ref 5]): "*Any type of recorder installed in the aircraft for the purpose of complementing accident/incident investigation.*" (ICAO Annex 6, Part I [Ref 6])
Flight recorders addressed in the present document include:

- Flight data recorders
- Cockpit voice recorders
- Data link recorders

[1] Regulation EU 2016/679 of 17 April 2017 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, article 4(7).
[2] Regulation EU 2016/679 of 17 April 2017 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, article 4(2).

- Flight crew-machine interface recorders

Flight recorder data (Ref. definition QR-FRD Study report D6 [Ref 5]): Any type of data recorded by the flight recorders that would be used for the purpose of complementing accident/incident investigation. Flight recorder data may include:

- Mandatory and optional flight parameters recorded by flight data recorders
- Audio recordings between the flight crew members and any other station
- Audio recordings of the acoustic environment of the cockpit
- Messages and information exchanged over data link
- Imagery from displays inside the cockpit and interactions of flight crew members with instruments and displays

Key (Public key infrastructure): Set of roles, policies, procedures, hardware and software needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption. It provides a confirmation of the identity of parties involved in the communication as well as the validation of the information being transferred.

In flight distress event (EUROCAE ED237 [Ref 39] definition)*: A situation which, if left uncorrected, is likely to result in an accident.*

Nuisance trigger (EUROCAE ED237 [Ref 39] definition)***:*** *Any trigger that is erroneously generated by the on-board triggering system when there is no potential for an accident.*

Serious incident (ICAO definition). An incident involving circumstances indicating that an accident nearly occurred. *Note 1. — The difference between an accident and a serious incident lies only in the result.*

Safety and security: as defined in doc. 9859 (Safety Management Manual) [Ref 12] section 2.1.1, within the context of aviation, **safety** is "*the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable leve*l". It must be distinguished from **security**, which relates to acts or attempted acts such as to jeopardize the safety of civil aviation. To be noted, this distinction between safety and security is used in aviation and in other domains involving operational risks. In a broader context, safety is one aspect of security[3].

Safety Management System: "A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures." (ICAO Annex 6 [Ref 6])

3.2 Acronyms

Acronym	Definition
ACARS	Aircraft Communication Addressing and Reporting System
ADFR	Automatic Deployable Flight Recorder
ADRS	Aircraft Data Recording System
ADS-B	Automatic Dependent Surveillance-Broadcast
AIAs	Accident Investigation Authorities

[3] For instance in the GDPR the words "*public security*" include "*the protection of human life especially in response to natural or manmade disasters*" (whereas 73).

Acronym	Definition
AIR	Airborne Image Recorder
AMS(R)S	Aeronautical mobile-satellite (Route) service
AISD	Airline Information Service Domain
ATC	Air Traffic Control
ATS	Air Traffic Service
BEA	Bureau d'Enquêtes et d'Analyses (French AIA)
CARS	Cockpit Audio Recording System
CFIT	Control Flight Intro Terrain
COI	Conflict of interest
CVR	Cockpit Voice Recorder
DAR	Direct Access Recorder
DLR	Data Link Recorder
DTSP	Data transmission service providers
EGPWS	Enhanced Ground Proximity Warning System (Honeywell)
EDPB	European Data Protection Board
FAA	Federal Aviation Administration (USA)
FCMIR	Flight Crew-Machine Interface Recorder
FDM	Flight Data Monitoring
FDR	Flight Data Recorder
GADSS	Global Aeronautical Distress & Safety System
GDPR	General Data Protection Regulation (European Union)
GEO	Geostationary Orbit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
ISO	International Standardization Organization
ITU	International Telecommunication Union
LEO	Low Earth Orbit
LOC-I	Loss of Control in Flight
MAC	Mid Air Collision
MEO	Medium Earth Orbit
MSS	Mobile Satellite Service (Inmarsat, Iridium)
NPA	Notice of Proposed Amendment
PIESD	Passenger Information and Entertainment Services Domain
QAR	Quick Access Recorder
SAR	Search and Rescue
SARPs	Standards and Recommended Practices (ICAO)
SRR	Search and Rescue Region
TAWS	Terrain Avoidance Warning System (ICAO term)
TCAS	Traffic Collision Avoidance System
VHF	Very High Frequency
VPN	Virtual Private Network

Table 1: Acronyms

4 Preliminary chapter

Until now, after an accident, the only way to transmit the flight recorder data to an AIA is by recovering, transporting, and delivering physical data recorders. This is done under supervision of States authorities as per ICAO Annex 13 Standards [Ref 8] and national regulations.

The future QR-FRD process completely changes this as two sources of recorded data (physical recorders data and transmitted data) will coexist. Both present process (physical recorders) and future QR FRD process will not exclude each other. They will operate in parallel.

In the QR-FRD process, recorded data will be digitally transmitted from an aircraft via space and/or ground communication segment to data repository which could be located in various places of the world and, finally, be made available to an AIA. The process will no longer be conducted only by authorities, as service providers will oversee data transmission, storage, and protection. There will be no handling of recorders and part of the process will be automatic.

The table below illustrates the main changes brought by the QR FRD process.

PRESENT PROCESS (PHYSICAL RECORDERS)	**FUTURE QR-FRD PROCESS**
• Data continuously acquired and stored on dedicated recorders located on board	• Data continuously acquired and stored on dedicated recorders located on board **AND** data acquisition, formatting and storage for transmission • Automatic digital detection of conditions that could lead to an accident through triggers or continuous “Gate-to-gate” transmission[4]. • Data transmission (air and space segment)• Off aircraft storage (space and/or ground)
• Accident notification to AIA	• Accident notification to AIA
• Data recorder retrieved and physically transported to AIAs • Data stored (in AIAs laboratories) • Data recovered from physical recorders (in AIAs laboratories)	• Data recovery
• **Investigation**	• **Investigation**

To be noted:

- "gate-to-gate" continuous transmission envisaged as Solution #1 will transmit routine flight data, most of them being not related to accidents/serious incidents at all;
- significant flight data and communications data are already transmitted and made available via ADS-B, VHF (ATC) and ACARS messages without any specific data protection. For instance, websites such as "Flight Radar 24" or "Live ATCNet" use some of these data.

First, this chapter aims to present the main legal framework applicable when an accident or serious incident occurs as per ICAO definition. More specific standards and regulations relevant to the QR-FRD project will be developed further in Chapter 5.

Second, this chapter presents the main accident categories and the possible influence of the setup type and location of the accident.

4.1 General legal framework

Even if ICAO Standards are not legally binding, they largely structure the legal framework. On a regional level, the main European regulations will be introduced as well as other important regional regulations. Finally, the implementation of ISO Standards and ISO certification of the different operators are common in the aviation sector and this study proposes to regard them as a part of the legal framework[5].

4.1.1 ICAO Standards

The ICAO legal framework is structured around the 1944 Chicago Convention and its 19 Annexes. The annexes include Standards and Recommended Practices (SARPs). Even the standards are not strictly legally binding but according to article 38 of the Convention, States that do not comply with them must notify the ICAO. As they are formulated in general terms, the annexes often refer to more detailed and technical manuals, helpful for their practical implementation.

4.1.1.1 Annex 6 "Operation Of Aircraft" and corresponding manuals

Annex 6 [Ref 6] is central to our study as it lists the crash protected flight recorders which are the FDR, CVR, AIR, DLR and for aircraft for which the application for type certification is submitted on or after 1 January 2023, the FCMIR (s. 6.3).

Annex 6 Part I Chapter 6 was recently modified to incorporate the concept of operations of the Global Aeronautical Distress & Safety System (GADSS) issued in 2017. This new system was developed by a working group tasked by the ICAO following the tragedies of AF 447 and Malaysia Airlines 370 to improve aircraft tracking to facilitate timely aircraft location, search and rescue operations and timely recovery of flight data.

As of today, section 6.3.6 on "Flight recorder data recovery" requires the following:

6.3.6.1 "All aeroplanes of a maximum certificated take-off mass of over 27 000 kg and authorized to carry more than nineteen passengers for which the application for type certification is submitted to a Contracting State on or after 1 January 2021, shall be equipped

[5] ISO standards were introduced in the QR-FRD Study D4.

with a means approved by the State of the Operator, to recover flight recorder data and make it available in a timely manner".

Appendix 8 of Annex 6 part I completes Chapter 6 on flight recorders as it gives general and specific requirements. But it applies for now only to physical flight recorders and may have to be completed to address the two solutions analyzed in this study. Requirement could be made on the collection, transmission, storage and recovery of data to ensure reliability of the process.

The most important corresponding ICAO Manual is doc. 10054 on Location of Aircraft in Distress and Flight Data Recovery [Ref 15]. It was published in 2019 to integrate the GADSS and a revised edition is expected.

At the time the present study was written, Doc 10165, addressing the four pillars of the GADSS concept, was under development. It is expected that Doc 10165 will replace Manual 10054.

Manuel 10054 gives a very broad definition of "*timely recovery*": "*as soon as possible*" or "*without unnecessary delays"* (section 3.3.2).

In Doc 10165 the definition of timely recovery has been modified to read "*Timely means as soon as possible for a specific situation, with a reasonable expectation of recovering the data on the order of days*."

As for the data considered, the Manual states that "the system for the timely recovery of flight recorder data has to provide, at a minimum, the data from the time the aeroplane enters the distress conditions to the end of the flight" (…) "Also, to the extent possible, historical data prior to the time the flight enters the distress conditions should be provided with the most recent data being given the highest priority. Nevertheless, the objective is to recover the complete contents of flight recorder data, in a timely manner" (section 3.3.4).

The State of the operator "may complements its regulations on the timely recovery of flight recorder data", "in line with ICAO Standards and this manual" (section 3.3.5).

The established policies and procedures should "specify how the data will be protected and provided to the AIA in charge of the investigation" and "include, at a minimum:

a) contracting minimum performance standards and quality of service (availability of services, advance notification of outages, and geographical coverage of planned, alternative and emergency flight routes);

b) data-capturing procedures ensuring the protection and integrity of information;

c) data retention and access control;

d) agreement on principles for granting the AIA in charge of the investigation access to the data".

The operator "should develop policies and procedures for third parties that perform work on its behalf" and as "flight recorders contain sensitive information; access should therefore be subject to restrictions" and refers to Annex 13 [Ref 8] for the use and protection of investigation records and related sources and Annex 19 [Ref 9] for the use of safety data and safety information as part of the safety management system (section 3.3.6.5).

4.1.1.2 Annex 10 "Aeronautical Telecommunications" and corresponding manuals

Annex 10 [Ref 7] is relevant on the issue of data transmission and particularly Volume III on Communication Systems and Volume V on Radiofrequency Spectrum Utilization.

Even though they do not expressly deal with the timely recovery of flight recorder data, both those volumes draw attention to the fact that the considered data transmission, as they will be added to the aeronautical communications already in place, will, like all the others, heavily rely on the availability of frequency spectrum and on satellite constellation capacities.

In a 2019 position paper issued at the World Radiocommunication Conference, the ICAO insisted on the protection of "aeronautical access to appropriately protected spectrum for radiocommunication and radionavigation systems that support current and future safety-of-flight applications. In particular it stresses that safety considerations require that adequate protection against harmful interference must be ensured"[6]. In this paper, item 1.10 deals with the necessity "to consider spectrum needs and regulatory provisions for the introduction and use of the global aeronautical distress and safety systems (GADSS)", which includes flight data recovery.

Further developments on the relationship between the ICAO and the International Telecommunication Union (ITU) regarding the protection of a dedicated radio spectrum and the satellite issue will be found at section 5.3.1.2.1.

The main ICAO manual on spectrum utilization is Doc. 9718 Handbook on Radio Frequency Spectrum for civil aviation (2nd ed. 2018) [Ref 10][Ref 10].

4.1.1.3 Annex 13 "Aircraft Accident and Incident Investigation" and corresponding manuals

Possible inconsistencies of Annex 13 [Ref 8] regarding the recovery of flight recorder data through systems that transmit data for storage off the aircraft have already been pointed out by ICAO's Accident Investigation Panel (AIGP) in May 2021. They were addressed during AIG/7 in May 2022 and will be reviewed by the Air Navigation Commission[7].

The AIGP were tasked to review Annex 13 and the new doc. 10054 [Ref 15] in relation to the GADSS "to ensure they are adequate for the protection of flight recordings in a "cloud" environment". The Panel noticed that "data transmission technologies create the potential for scenarios in which the flight recorder or flight recorder data may be held by one or more States not participating in the accident or incident investigation" and that "for aircraft equipped to transmit flight recorder data, this data will normally be transmitted to the air carrier through the communication service used by the carrier. In-flight transmission of flight recorder data will likely be involved satellites or/and multiple ground stations, with the received data transmitted and stored in a cloud environment. As a result, there may be full or partial electronical copies of the flight recorder data available in different States, including States not participating in the accident investigation".

[6] https://www.icao.int/ESAF/Documents/meetings/2017/IIM%20SUB%20GROUP%202017/Working%20Papers/APPROVED%20ICAO%20Position%20for%20the%20ITU%20WRC%2019.pdf

[7] ICAO, Accident Investigation Panel (AIGP), « Proposed Amendments to Annex 13 and guidance material regarding recovery of automatic deployable flight recorders and protection of transmitted flight recorder data », 6th meeting, 10-21 May 2021, AIGP/6-WP/16. The May 2022 AIG/7 meeting's report is not yet available.

To address those situations, the panel considers as relevant section 5.14 and 5.16 of Annex 13:

5.14 “Any State shall, on request from the State conducting the investigation of an accident or an incident, provide that State with all relevant information available to it”.

5.16 “When an aircraft involved in an accident or a serious incident, lands in a State other that the State of Occurrence, that State of Registry or the State of the Operator shall, on request from the State conducting the investigation, furnish the latter State with the flight recorder records and, if necessary, the associated flight recorders”.

The Panel considers that rather than adding new protections, the modification of Annex 13 should give similar protection to transmitted flight recorder data. To do so, the Panel recommends the revision of the definition of flight recorders, so that it includes “*systems that transmit data for storage off the aircraft for the purpose of complementing accident/incident investigations*” and the creation of a new Standards that “*must ensure that any full or partial electronic copies of transmitted flight recorder data are provided to the State conducting the investigation without requiring a request*”.

Flight recorders would indeed be defined as “any type of recording system installed in the aircraft for the purpose of complementing accident/incident investigations, including systems which transmit data for storage off the aircraft”.

And a new section 5.14.2 would provide that “*If a State has availability to any data from a flight recorder of an aircraft involved in an accident or incident, that State, a) shall, without delay, provide that State conducting the investigation with all such data available to them; and b) shall not divulge such data without the express consent of the State conducting the investigation*”.

Finally, the work of the AIGP/4 group has resulted in the introduction of a new provision in Annex 13. Section 5.8 now provides that: "*Effective use shall be made of available ground-based recordings in the investigation of an accident or an incident*.”. A State Letter of 14 March 2019 (AN 6/1.2-19/12) points out “*that additional benefit of this new provision would be the inclusion of the so-called “cloud-based” flight data recordings on computer servers on the ground*.”.

If those modifications are to be incorporated in Annexes 13 and 6, it will lead to correlative modifications of Doc. 9756, Manual of Aircraft Accident and Incident Investigation [Ref 11], as it deals with flight data recorders in its chapters 6 and 7.

Another important provision is section 5.12, which provides that “*The State conducting the investigation of an accident or incident shall not make the following records available for purpose other than accident or incident investigation (…)*”. The CVR and AIR and their transcripts are in the scope of this section. For the FDR similar provisions exist in section 3.3.5 of Annex 6.

Regarding that section, Doc. 10054 (already mentioned for Annex 6) [Ref 15] directly links this State requirement to the “*means used for transmitting data from the aeroplane to the secure server*” (section 3.6.1.1). Those means “*are expected to include data encryption and signing techniques to ensure the protection and the integrity of the data*”. Therefore “*the State of the Operator will ensure that the operator has developed appropriate policies and procedures to ensure the protection of safety information*”. The Manual therefore places an obligation on States to ensure the Operators implement the right techniques for the protection of safety information.

Doc. 10054 adds that "*while services such as the secure data transmission from the aeroplane to the ground and the storage of the flight recorder data may be available, operators have to be made aware that they remain fully responsible for protecting these data against unauthorized access and for providing unaltered and unprocessed data to the appropriate authorities*" (section 3.6.2.1) and that "*hence, an operator is expected to carefully consider the guarantees offered by such services before subscribing to them (…)*" (section 3.6.2.2).

Furthermore, Doc. 10054 contains numerous provisions that will be further studied for each functional blocks: on the careful selection of service providers by the operators, on the safe custody of data, on the minimum duration of the transmission of data after a distress event, etc.

Another important corresponding manual is Doc. 10053, on Protection of Safety Information [Ref 13]. Its section 2.3.3 stresses that "an adequate legal framework should include provisions for the appropriate use and protection of the investigation recorders, including how to deal with public disclosure".

4.1.1.4 Annex 19 "Safety Management" and corresponding manuals

In principle, the QR-FRD project only deals with accidents (as per ICAO Annex 13 definition). However, per design and whatever the solution will be (continuous, triggered or hybrid), QR-FRD systems will transmit flight data for other reasons than accident. That explains why this report will present and discuss the main standards in Annex 19, applicable to data collected for the purpose of Safety Management.

Annex 19 is relatively new (1st ed. 2013; 2nd ed. 2016 and 3rd ed. 2019) [Ref 9] and aims at consolidating and reorganizing pre-existing Standards and Recommended Practices (SARPs) dedicated to accident prevention and placed in various Annexes.

The relevant part is Chapter 5 on Safety Data Collection and Processing Systems. It refers to Annex 19 Appendix 3 which gives "*principles for the protection of safety data, safety information and related sources*". Protection of safety data is indeed "*essential to ensure their continued availability*".

The corresponding manual is Doc. 9859, the Safety Management Manual (4th ed. 2018) [Ref 12]. Its Chapter 5 also deals with Safety Data Collection and Processing Systems. It deals with the quality of data and with Data Governance (section 5.5.4), defined as "*the authority, control and decision-making over the processes and procedures that support an organization's data management activities*". The main characteristics of data governance should be: integrity, availability, usability and protection. Those principles are relevant for our study.

4.1.2 Data regulations: the GDPR as a "Gold Standard"

The implementation of QR-FRD requires a review of various regulations concerning data and especially personal data. The legal status of the data considered for the QR-FRD study will be considered in more details in chapter 5, at the stage of data collection (FB1, section 5.1).

The study has concluded that the essential data regulation to be considered for the QR-FRD system will be the EU General Data Protection Regulation (GDPR, Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

persons with regard to the processing of personal data and on the free movement of such data) [Ref 23].

Indeed, its wide definition of personal data and extensive territorial scope make it unavoidable, even outside Europe.

Article 4 of the GDPR makes it applicable to data that allows to identify a natural person, even indirectly, "in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity".

CVR and FCMIR record personal data but some of the FDR parameters can also be regarded as personal if they allow to identify the actions or omissions of the aircraft's flight crew.

A natural person is considered "identifiable" if his or her identification does not require unreasonable time, effort, or resources[8]. As long as the pilots' positions are known, even anonymous FDR data can be regarded as personal for the purpose of GDPR application. Given the practical difficulty of discriminating between technical data that allows such identification and data that does not, and apply different standards to them, it seems appropriate and advisable to consider the GDPR as the "Gold Standard" applicable to the whole QR-FRD system and apply its protective measures to the entirety of the Flight Recorders Data.

Regarding territorial scope, article 3 of the GDPR gives two main criteria for its territorial scope. It applies:

- "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not";
- "to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (…) the monitoring of their behavior as far as their behavior takes place within the Union".

As a result, the GDPR applies outside Europe, which confirms its position as the main legally binding standard to be considered for data protection in the context of our study. The content of this protection will be analyzed at section 5.1.2.

It should also be noted that the GDPR relies on certification mechanisms set up by accredited certification bodies for the purpose of demonstrating the Controller's and Processor's compliance (articles 42 and 43). Our study has concluded that certification should be ensured through ISO Standards which are therefore considered in this document as part of the legal framework.

Specifically, regarding the concepts of Controller and Processor in the GDPR, the European Data Protection Board (Guidelines 07/2020) as well as the ECJ provide a clear view of who is the processor and controller at all stages of the process:

[8] This is the case, for example, when the identification of the data subject requires excessively complex, time-consuming, and costly operations. What constitutes unreasonable time, effort or resources should be considered on a case-by-case basis, taking into account factors such as the purpose of the processing, the cost and benefits of identification, the type of controller and the technology employed.

- The concept of controller is a functional one: "the legal status of an actor as a "controller" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being the controller" (EDPB Guidelines 07/2020 para 12).
- According to that functional concept, airlines will be the main data controllers, even if they do not have access to the data processed (on the fact that the access to the data by the controller is not necessary, see: ECJ – GC – 5 June 2018, Wirtschaftsakademie, C-201/16).
- But, as soon as the AIA has collected and starts to process the data for its own purposes, it becomes a controller according to the functional approach, and must comply with the GDPR unless the law has set some derogations (e.g. data minimization, data access limitation during the investigations...) - this has been confirmed by the ECJ in a recent case for a state tax authority : Valsts ienemumu dienests, 24 February 2022, C-175/20.
- There can be no joint controllership between the companies and the AIAs as they will act as successive controllers (joint controllership only applies when the processing by each party is inseparable).

4.1.3 Relevant EU Regulations

Regulation EU 996/2010 on the investigation and prevention of accidents and incidents in civil aviation [Ref 20][Ref 20] is of course of the utmost importance as it incorporates most of the Annex 13 Standards and Recommendations.

Its Recital 29 advocates for research on the possibility of accessing flight recorder information without the flight recorder being physically present.

Some of this Regulation's provisions may need to be revised prior to enforcing the QR-FRD:

- Article 6 on "*Cooperation between safety investigation authorities*" could be amended to specify that the State which has access to the data should provide without delay the data to the State conducting the investigation and should not divulge such data without the express consent of the State conducting the investigation.

- Article 8 on the "*Participation of EASA and national civil aviation authorities in safety investigations*" could include a provision specifying that the participants to a safety investigation (the safety investigations authorities, EASA, national civil aviation authorities of the Member States concerned, Accredited Representatives) are entitled to access to QR-FRD data. It would complete provisions such as the possibility to "*receive copies of all pertinent documents*" (article 8(2)(c)) but should also include the limitation of article 8(2)(d) which entitles them to "*participate in the read-outs of recorded media, except cockpit voice or image recorders*".

But it also appears that, contrary to Annex 13 [Ref 8], some of Regulation 996/2010 provisions refer to "recordings" and not only to "recorders", which could allow to interpret them as already applying to QR-FRD data:

- Article 11 on the "*Status of safety investigators*" already deals with recordings and is not limited to recorders as it provides that the investigator-in-charge is entitled to: "*…(c) have immediate access to and control over the flight recorders, their contents and any other relevant recordings*", a wording that seems sufficient to include QR-FRD recordings.

- Article 13 on "*Preservation of evidence*" also refers to recordings: "*any person involved shall take all necessary steps to preserve documents, material and recordings in relation to the event, in particular so as to prevent erasure of recordings of conversations and alarms after the flight*".
- Article 14 (2) on "*Protection of sensitive information*" provides that "*flight data recordings shall not be made available or used for purposes other than those of the safety investigation (…)*".

Finally, the definition of "flight recorder" in article 2(6) could be amended in a way similar to the AIGP's proposed amendments to Annex 13 Instead of "*any type of recorders installed in the aircraft for the purpose of facilitating accident/incident safety investigations*" flight recorders could be defined as "*any type of recording system installed in the aircraft for the purpose of complementing accident/incident investigations, including systems which transmit data for storage off the aircraft*".

Regulation EU 376/2014 on the reporting, analysis, and follow-up of occurrences in civil aviation links accidents and safety hazards [Ref 22]. Recital 5 states that "*experience has shown that accidents are often preceded by safety-related incidents and deficiencies revealing the existence of safety hazards. Safety information is therefore an important resource for the detection of potential safety hazards*". This regulation supports key parts of the Safety Management Systems.

Regulation EU 2018/1139 on common rules in the field of civil aviation and establishing the European Union Aviation Safety Agency [Ref 24] requires, at article 30 (7) that aircraft shall be equipped with necessary safety related equipment, including some **or** all the following… "*Means to recover flight recorder data in a timely manner in case of aircraft in distress by relying on real-time electronic communication or other appropriate technical solution*".

4.1.4 ISO Standards

In order to demonstrate that actors are compliant with the GDPR, the certification is encouraged.

Indeed, according to Article 42 of the GDPR: "*The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.*

In addition to adherence by controllers or processors subject to this Regulation, ***data protection certification mechanisms****, seals or marks approved pursuant to paragraph 5 of this Article* ***may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation*** *pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via*

contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects."

As the GDPR is an essential standard to implement the QR-FRD (see above), certification is a way to ensure its application even in cases where it would not otherwise be strictly applicable.

Reference to ISO standards is a well-known method, already used in several ICAO standards:

- Annex 3 "Meteorological Service for International Air Navigation" recommends to be ISO 9000 "Quality management systems" certified in order to comply with the requirement to provide an efficient meteorological data processing procedure, (paragraph 2.2.3);
- Annex 10 "Aeronautical Telecommunications" provides that the ATS messaging service is implemented according to the specifications of ISO standards, the 10021 package.;
- Annex 15 "Aeronautical information services" refers to ISO standards in its definitions, including ISO 8601, ISO 9000 and the ISO 10100 package.

More generally, the ICAO participates in the development of certain standards within the ISO. Both organisations are therefore known to each other.

ISO standards, as an international reference, are therefore relevant to our study, especially at the stage of data transmission (FB3) and Data storage (FB4).

ISO are organized in "packs" or "families" and the main relevant is Pack 27000 which deals with information security[9]. Standard 27701 includes a cross-reference table to show how compliance with the requirements of this standard may be relevant to meeting the requirements of the GDPR.

4.2 Accident scenarios

This section deals with the three most relevant accident categories, when recorded data cannot be quickly recoverable and study the possible influence of the accident location.

4.2.1 Possible influence of accident setup types

As explained above, Annex 6 Part I, para 6.3.6.1 [Ref 6] has been modified and now recommends aeroplanes to be equipped "with a means (…) *to recover flight recorder data and make it available in a timely manner."*

This can be obtained by Automatic Deployable Flight Recorder (ADFR) presently tested to be certified on future aircraft types (A350 for instance) and by recorded data transmission devices addressed in the present QR-FRD study. Presence of both systems on the same aircraft must be envisaged here.

Safety occurrences to be considered are "accidents" which require an Annex 13 investigation and result in flight recorders not being quickly recoverable.

This excludes the following occurrences where recorded data can be made "*available in a timely manner*" by using directly physical data recorders at an airport:

[9] See QR-FRD Study D4.

- incident and serious incident;
- accident in flight followed by a landing on an airport;
- accident located on an airport.
- Therefore, the following three main accident categories remain:
- Loss of Control in Flight – LOC-I;
- Controlled Flight Into Terrain – CFIT;
- Mid-air collision – MAC.

Most of these accidents are catastrophic (great number of fatalities, aircraft destroyed).

To be noted: LOC-I, CFIT, MAC accidents located close to an airport do not mean that recorded data will necessarily be « *made available in a timely manner* ». Data recorders have sometimes proved difficult to locate and retrieve after impact in mountainous areas or in water, even shallow.

In theory, only flight recorder data in relation with these categories must be considered. However, the present QR-FRD study has shown that recorded data necessary to perform the investigations cannot be transmitted instantly, at the very moment of occurrence. The transmission of flight recorder data needs to be initiated before the occurrence is certain. Therefore, data will be transmitted even in the absence of any accident, either through continuous transmissions (solution # 1 of the study), or through triggered transmissions when specific conditions very similar to a near accident are met (solution #2).

4.2.1.1 Loss of Control in Flight (LOC-I)

Loss of control in flight (LOC-I): an extreme manifestation of a deviation from intended flightpath.

This accident category may happen at any time during the flight. At low height, the scenario can last a few tens of seconds before the impact. When the loss of control begins during cruise the scenario can last several minutes. The AF447 loss of control lasted more than 4 minutes between the initial aerodynamic stall and the impact.

For simplification, when they result ultimately in a loss of control and an impact, the following accident scenarios listed in the CAST/ICAO Common Taxonomy Team (CICTT) document are considered as LOC-I[10] :

- Fire/Smoke (Non-Impact) (F–Ni);
- Fuel Related (Fuel);
- Icing (Ice);
- System/Component Failure Or Malfunction (Non-Powerplant) (Scf–Np);

[10] See the matrix provided in the QR-FRD Study D1 [Ref 1], “Accident categories (CICTT) and in the QR-FRD Study D3 and appended tables.

- System/Component Failure Or Malfunction (Powerplant) (Scf–Pp);
- Turbulence Encounter (Turb);
- Wind Shear Or Thunderstorm (Wstrw).

In case of partial loss of control events when the crew recovers the aircraft control, recorded data will be made available after landing, directly from physical recorders and from data transmission (continuous or triggered).

Some LOC-I scenario may last more than several tens of a minutes. Questions regarding the location of occurrence may be raised as a significant distance may be flown between the loss of control and the impact.

4.2.1.2 Control Flight Into Terrain (CFIT)

Controlled Flight Into Terrain (CFIT) : In-flight collision (or near collision) with terrain, water, or obstacle without indication of loss of control.

Most CFIT accidents related to aircraft types involved in this study happen during departure or arrival phases.

In solution #2, recorded data transmission will be typically triggered at the activation an Terrain Awareness and Warning System (TAWS). In most of the case, pilots react to TAWS warnings by correcting the flight path and the CFIT is avoided. Depending on reaction time and obstacle clearance margin, this scenario may correspond to a serious incident and lead to an Annex 13 investigation. Here again, recorded data related to a near CFIT events will be made available after landing directly from physical recorders and from data transmission (continuous or triggered).

For Solution #2, in case of a real CFIT accident, the time available before the impact to transmit recorded data when trigger conditions are met is less than a few tens of seconds.

4.2.1.3 Mid-Air Collision (MAC)

Mid-air collision (MAC): all collisions between aircraft while both aircraft are airborne.

Per definition a MAC accident involves two aircraft. This type of accident is very rare. When it happens, the result is generally a total loss of both aircraft but not always. Some may lead to the loss of only one aircraft or even no loss at all, only damages.

The time available to transmit recorded data when trigger conditions are met is a few tens of a second when based on ACAS equipment (TCAS II) alert (i.e. Resolution Advisory). But for different reason, a collision may happen without advanced warning (ACAS system malfunction, collision with light aircraft without transponder etc.).

ATC's very first mission being aircraft separation, ATC data plays a greater role for MAC investigations than for LOC-I and CFIT accidents. Relevant ATC data is recorded: Aircraft/ATC communications and recorded radar data. The public has access to part of this data through radio receivers or internet platforms such as Flight Radar 24 which give an access to ADS-B data (altitude, position, ground speed etc).

Unlike CFIT and LOC accidents, MAC accidents may initially involve two AIAs which may legitimately claim responsibility for the investigation when the accident occurs in an international airspace and the aircraft are registered in two different countries.

4.2.2 Possible influence of Accident locations

The EASA consultation required this report to address the possible influence of accident locations.

The first consequence that introducing QR-FRD will have is that access to Flight Recorder Data will no longer be related to the accident location.

In fact, regardless of whether the accident took place within the EU, over a non-EU member State, outside any national airspace (for instance over the ocean) or even in a State that, for whatever reason, is not willing to investigate (for instance if it is not a party to the Chicago Convention or if it is simply uncooperative), access to the Flight Recorder Data will not be affected: access to the data and access to the accident site will no longer be related. From that point of view, the introduction of QR-FRD may seem a progress.

This could lead to a reflection on the criteria set forth in Annex 13 for the determination of the competent AIA. Under the present standards, the responsibility to conduct the safety investigation lies primarily with the State of occurrence's AIA[11]. As an exception, that responsibility can be transferred to the State of registry's AIA when:

- the State of occurrence is not a party to the Chicago convention and does not intend to conduct the safety investigation in accordance with Annex 13[12] ; or
- when the accident location "cannot definitely be established as being in the territory of any State"[13], for instance when the accident took place outside any national airspace, or when it has not been possible to locate the aircraft.

The fact that the State of occurrence will no longer be the one having the easiest access to Flight Recorder Data could lead to wonder whether it would make sense to amend these criteria.

Maintaining a preference for the State of occurrence's AIA is however justified by other reasons:

- immediate access to the accident site will still be of primary importance to gather evidence, retrieve data from the physical flight recorders, examine the aircraft or its wreck, conduct medical examinations, identify and interview witnesses…
- the State of occurrence's AIA is the best equipped to liaise with the local judicial authorities who will generally have jurisdiction to launch judicial investigations.

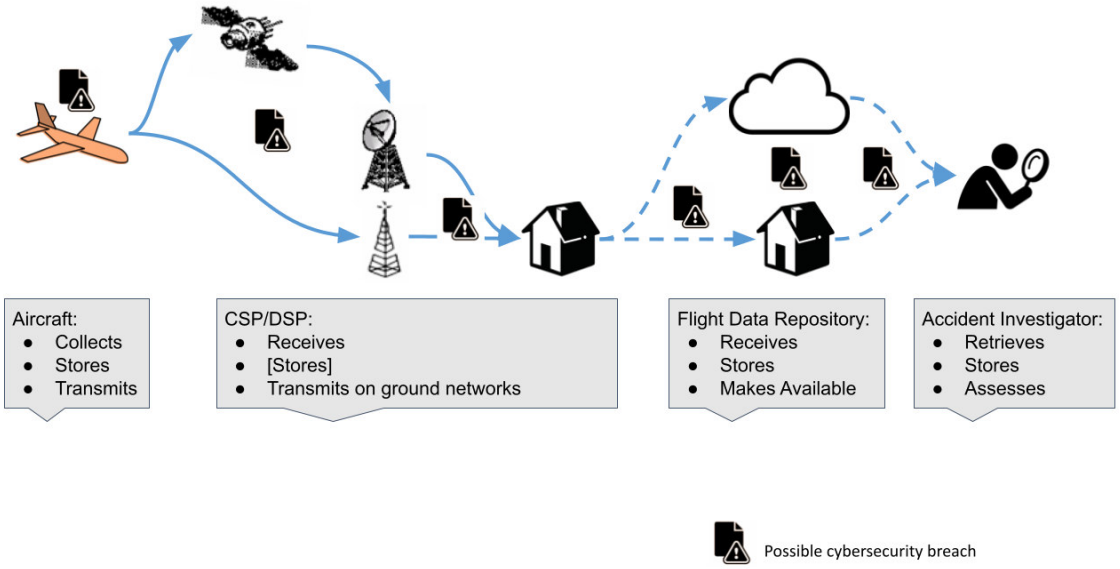
[11] ICAO Annex 13, section 5.1.
[12] ICAO Annex 13, section 5.2.
[13] ICAO Annex 13, section 5.3.

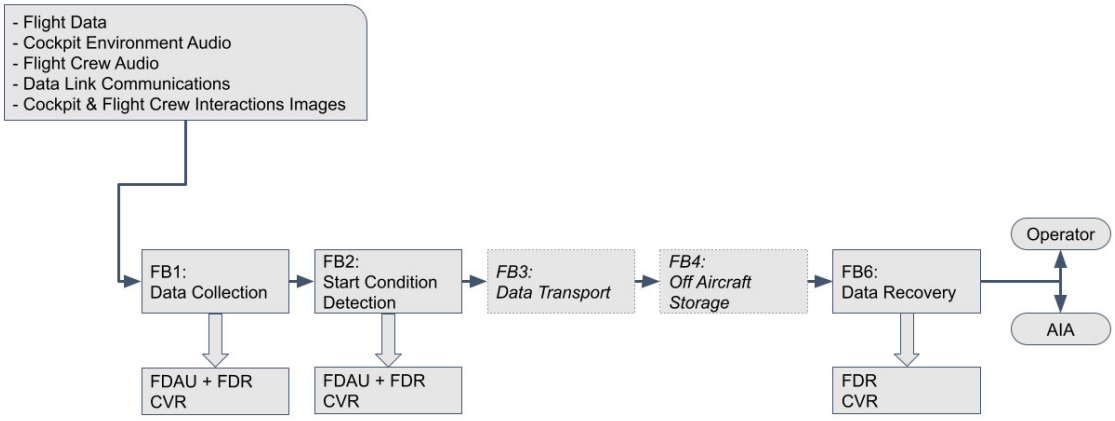
5 Legal framework applicable to both technical solutions

This chapter will review the legal framework applicable to actors (airlines, AIAs, transmission service providers, data recipients…) and assets (satellite, ground station…) involved in the quick recovery of flight recorder data. It will do so by focusing on each of the functional blocks (FBs) identified in report D2 [Ref 2] and will identify, at each step, what legal issues may arise (*possible inconsistencies with ICAO Annex 13, legal uncertainties and risks for the protection of flight recorder data)*, and suggest ways to resolve them.

Unless specified otherwise, the legal issues analyzed in this chapter apply in the same way for both technical solutions #1 and #2. Only a few issues appear to be specific to either of the two solutions, as will be mentioned when examining them.

The two following figures illustrate the QR-FRD process. The second figure shows the functional blocks used in previous reports and adopted in this legal study.





5.1 FB1 – Data collection / Acquisition and Digitization

At the stage of data collection, two legal issues arise: the issue of data ownership and the protection of personal data.

5.1.1 Is there a Data Ownership?

The data transmitted to the AIAs must be "*unaltered and unprocessed*"[14] and in principle, raw data is not subject to any property rights as it is not legally considered as an appropriable asset.

But even though the QR-FRD deals with unprocessed data, the fact that it is collected and/or organized in a systematic way for the purpose of storage and transmission to the AIA could raise the question or whether it constitutes a database.

Databases can be protected under certain regulations[15], notably if they are an original intellectual creation or if the database maker is able to justify a "*substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*"(Directive 96/9/C, article 7 [Ref 26]).

However, even if some airlines claimed that the "substantial investment" they spent to obtain the records gives them specific rights over the data, this could not prevent the use of QR-FRD for safety investigations purposes:

- article 9 of Directive 96/9/C [Ref 26] itself allows to extract and use the data without authorization of the database's maker "*for the purposes of public security*" (which in this Directive encompasses safety)
- the duty to make the data available to the AIA is enshrined in ICAO Annex 6 [Ref 6], section 6.3.6.1 and in Manual 10054 [Ref 15], section 3.6.3.2
- similarly Regulation (EU) 996/2010 [Ref 20], article 11(2)(c) provides that the investigator-in-charge is entitled to "*have immediate access to and control over the flight recorders, their contents and any other relevant recordings*".

The study has therefore reached the conclusion that any ownership claims over the data, even assuming that they were successful, would be very unlikely to prevent AIA's access and hinder the investigations.

[14] ICAO Manual doc. 10054, section 3.6.2.1.

[15] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, which defines data bases as "*a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronics or other means"*

5.1.2 Personal Data

In EU law, the protection of personal data is recognized as a fundamental right embodied in Article 16 of the Treaty on the Functioning of the EU and Article 8 of the Charter of Fundamental Rights of the EU. The GDPR [Ref 23][Ref 23] guarantees a high level of protection. It has been described as the "*toughest privacy and security law in the world*"[16].

As already explained (see 4.1.2) the GDPR's extraterritorial scope advocates for the application of its principles to all Flight Recorder Data.

However, it is worth mentioning Convention 108 of the Council of Europe *"for the Protection of Individuals with regard to Automatic Processing of Personal Data"* (1981) as the first internationally legally binding act dealing with data protection, ratified by the 47 Council of Europe Member States including for instance the Russian Federation. A modernized version of the Convention will enter into force on 11 October 2023 with a level of protection similar to the GDPR.

Many countries, on the other hand, do not recognize a general right to personal data protection, including major nations such as the USA. The question of the compatibility between US and EU laws[17] as well as between Chinese and EU laws[18] is not settled.

As was seen in section 4.1.2, the definition of "personal data" in the GDPR is very broad as it relates to both identified and identifiable natural persons ('data subjects'). The identification of a natural person can therefore be made from a single data or from the crossing of a set of data.

According to that definition, even technical data such as some of the FDR parameters can be regarded as personal if their crossing with other data allows to identify the actions or behavior of a crew member for instance.

The principles relating to the processing of personal data are outlined in article 5 of the GDPR. Among them, transparency, purpose limitation, data minimization, storage limitation, integrity and confidentiality.

As for the data subjects' privacy rights, the list includes the right to be informed, the right of access and to obtain a copy, the right to rectification, to erasure and to restrict processing. Some of these rights may not be exercised fully when an accident or serious incident occurs as ICAO Annex 13 [Ref 8] limits the availability and disclosure of recorded data[19], but article 23 of the GDPR allows to restrict the scope of these obligations and rights by adopting a law

> "*when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard : (…)*
>
> *(c) public security*

[16] https://gdpr.eu/tag/gdpr/?cn-reloaded=1

[17] https://www.cnil.fr/sites/default/files/atoms/files/declaration_01-2022_du_cedpb_sur_lannonce_dun_accord_de_principe_sur_un_nouveau_cadre_transatlantique_pour_la_protection_des_donnees.pdf

[18] On 20 August 2021, China adopted its first unified data protection law. A major difference with the GDPR relates to international data transfers. In addition to guarantees similar to those provided for by the GDPR, that law makes the transfer conditional upon a prior security analysis. It also tends to limit cross-border data transfers by imposing data storage on Chinese territory, except with specific authorization from the State Department.

[19] ICAO Annex 13, section 5.12.

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e)[20], which includes public security (the "official authority" may be AIAs).

This restriction applies when an accident or serious incident occurred, and an AIA is investigating[21].

If an accident or serious incident did not occur, the question of the protection of the collected data remains.

Solution #1 therefore raises more concerns in respect of compliance with the GDPR than does solution #2. In solution #1, data, including personal data, are acquired, transported and stored systematically, regardless of their potential relevance for an AIA investigation; indeed, an overwhelming majority of flights are performed without accidents or serious incidents, which could lead to the conclusion that in that vast majority of cases, the collection of personal data will notbe lawful.

This, however, would be an erroneous conclusion. As rare as they may be, instances when flight recorders cannot be physically recovered have been determined to be sufficient reason to mandate quick recovery of data through other means. If solution #1 were to be pursued, its primary purpose would remain to allow for the investigation of accidents and serious incidents and thereby ensure aviation safety.

Robust encryption (see paragraph 5.1.3) and limited time of storage policies (see paragraph 5.4.3) should however be very strictly implemented.

Finally, regarding non personal data, EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union requires that it should be available for competent authorities (article 5); and, mirroring the public security exception for personal data (see above), it prohibits data localization requirements "*unless they are justified on grounds of public security in compliance with the principle of proportionality*" (article 4(1))[22].

5.1.3 Ensuring the protection and integrity of the data by robust procedures

General standards and obligations can be found in the ICAO Manual doc. 10054[Ref 15], in the GDPR [Ref 23] and in ISO Standards. They all advocate for the use of encryption technique.

QR-FRD study D2 [Ref 2] suggests that "*flight recorder data shall be protected over the whole end-to-end process, from their recording onboard the aircraft to their recovery by the accident investigation authorities and airlines operators, via the transmission over the air and through ground networks*"

[20] See definitions section, definition of « safety » and « security » in the context of aviation and the broader meaning of security in other contexts, which includes safety.

[21] Regarding this issue, there is no existing case law or official opinion. Before enforcing the QR-FRD system, it would be advisable to consult the European Data Protection Board (as permitted by article 64 of the GDPR).

[22] The Regulation 2018/1807 defines "*data localisation requirements*" as "*any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State (…) which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State*" (article 3(5)).

Study D2 indicates that VPN can only ensure data integrity/authenticity at the transmission level and of the air-to-ground segment and that encryption alone ensures confidentiality but not authenticity. Therefore, the QR-FRD study has proposed to combine encryption with digital signature to ensure protection and integrity throughout the whole process (see QR-FRD study reports D2, D3 [Ref 3] and D4 [Ref 4]). To that end, a policy on the holding of decryption keys will have to be defined (see section 5.5.5).

The blockchain: apart from VPN and encryption techniques, the blockchain has been considered not only as a data storage tool (see below, section 5.4.2.2.1), but also as an authentication system complementary to the data encryption itself (authentication of the data and timestamping). But other simpler and less expensive technologies can achieve the same result.

5.1.3.1 The ICAO Manual doc. 10054

This manual [Ref 15] insists on the liability of the operators regarding data encryption as they bear the responsibility to provide the AIAs with untampered data and decryption tools. Robust procedures and policies should be implemented as they must prevent man-in-the-middle attacks and service providers should be carefully selected.

Article 3.3.6.2 provides that “where the flight recorder data recovery system includes transmission from the aeroplane, the policies and procedures should include, at a minimum: (…) b) data-capturing procedures ensuring the protection and integrity of information; (…)”.

Article 3.6.1.2 specifies that “the means used for transmitting data from the aeroplane to the secure server are expected to include data encryption and signing techniques to ensure the protection and the integrity of the data” and article 3.6.1.3 insists on the fact that “one potential solution to prevent man-in-the-middle attacks is to implement robust procedures and policies for the management and protection of encryption keys shared between the airborne equipment transmitting the flight recorder data and the secure servers”.

Finally, article 3.6.1.4 states that “the State of the Operator will ensure that the operator has developed appropriate policies and procedures to ensure the protection of safety information and, in particular, to ensure that in case of an accident, the AIA in charge of the investigation retains full control over access to and use of flight recorder data in a usable (decrypted) format”. Indeed, according to article 3.6.2.1, “operators have to be made aware that they remain fully responsible for protecting these data against unauthorized access and for providing unaltered and unprocessed data to the appropriate authorities”. “Hence, an operator is expected to carefully consider the guarantees offered by such services before subscribing to them” (article 3.6.2.2).

5.1.3.2 The GDPR

The GDPR [Ref 23] insists on the necessity to secure the processing of personal data and encryption is one of the appropriate measures deemed to ensure a level of security appropriate to the risks.

Article 32(1) of the GDPR on security of processing, provides:

“1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of carrying likelihood and severity for

the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (…)".

5.1.3.3 ISO Standard 27002

The ISO Standard 27002 on Information Technology (Security Techniques – Code of practice for information security controls) [Ref 33] looks at encryption measures at section 10.1 and how they should be elaborated. Among various recommendations, the ISO states that the elaboration of an encryption measure should be risk-based: the level of protection needed will determine the type, power and quality of the encryption algorithm. The fact that the data are to be transferred and communicated is an important criterion for the encryption measure too.

The service provider must also elaborate a management policy for the encryption keys.

The ISO Standard recalls that the question of cross-border data flow and the potentiation application of various national laws must be considered. To that effect, section 18.1.5 recommends that the service provider should ask for legal advice before the communication of encrypted data when outside of its jurisdiction.

5.2 FB2 – Trigger Detection

This issue is of course specific to technical solution #2.

5.2.1 Selecting the proper triggers

To ensure that AIAs access all the necessary data, including all the FDR parameters listed in Appendix 8 to Annex 6 [Ref 6], the selection of events that will activate transmission must not vary from one operator to the other but will have to be harmonized.

Triggers necessarily depend on the type of aircraft. It should be the aircraft manufacturer's responsibility to set them for each specific aircraft type at the stage of aircraft type certification, thus allowing the certifying authority to oversee that selection.

EUROCAE has adopted a specification [Ref 39] for the selection of the relevant criteria, which ICAO Manual 10054 [Ref 15] recommends to use as a minimum list, however recommending "*that the manufacturer consider additional events (e.g. cabin depressurization, fire warning, terrain collision avoidance system..) beyond those described in EUROCAE ED-237 to ensure that an adequate amount of flight recorder data is transmitted*" (Manual 10054, section 3.6.13.5).

EUROCAE ED237 [Ref 39] Chapter 3 provides guidance for selecting relevant triggering criteria, such as:

- The occurrence of pre-defined scenarios;

- The minimum occurrence duration of a particular condition of a scenario (the persistence time);
- The detection of "return to normal" to allow automatic cancellation.

Overall "*the set of triggering criteria should maximize the detection of scenarios, while limiting nuisance triggering. Excessive nuisance triggers have the potential to reduce confidence in the system as well as saturate SAR resources*".

5.2.2 Other ICAO requirements

Section 3.6.13 of ICAO Manual 10054 [Ref 15] includes further requirements:

- data transmission should start as early as possible (ideally "*as soon as the aeroplane is able to move under its own power*") and at a minimum when the aircraft is in distress; it should then start "*immediately or no later than five seconds after the detection of the distress conditions*" (3.6.13.8);
- transmitted data must include historical data "prior to the time the flight enters the distress conditions (…) with the most recent data being given the highest priority" (3.6.13.7)

Some national regulations may require the possibility to remotely activate transmission from a ground station[23], but that requirement is not incorporated in ICAO standards.

5.2.3 Cases study

The EUROCAE ED237 [Ref 39] which supports the trigger concept addressed in this QR-FRD study refers to "*distress situation*" as a "*situation which, if left uncorrected, is likely to result in an accident*". Strictly speaking, on every flight, many situations managed by the flight crew meet this definition. More realistically EUROCAE's ED237 specification refers to "unusual" aircraft states related to attitude, speed, altitude etc. which represent conditions that could lead to an accident.

On board alerting systems play a very similar role when triggering cockpit warnings for the flight crew. These systems have been certified for decades and continuously been improved to limit drastically nuisance warnings.

5.2.3.1 The AF447 accident case[24]

Based on the BEA investigation report, the AF447 accident results from a loss of control due to an aerodynamic stall.

Stall warnings systems and, depending on aircraft types, flight envelope protection systems are in place to initiate recovery maneuvers and prevent stall situations. On aircraft equipped with flight protection systems the maneuver is automatically performed when specific conditions are met.

[23] Which may require the flight crew's consent if personal data is concerned (section 3.6.13.6).
[24] https://bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf

When flight envelope protections are absent, fail or do not play their role, stall warnings remain available to alert the flight crew who must initiate an immediate recovery maneuver.

Certification requires stall warnings systems to be designed with a sufficient margin between their activation and the actual stall to give the pilots enough time to initiate and perform a successful recovery maneuver.

To be credible and fulfill their alerting role, stall warnings must activate only when needed. Therefore, the precisely defined activation margins result from a trade-off between, on one side, the risk of having too many useless activations in daily operations and, on the other side, much less warnings with the risk of letting the pilots with not enough time to initiate the recovery maneuver.

Cockpit warnings and QR-FRD triggers deserve to be compared and, possibly, to be jointly addressed.

Both need to be submitted to high-level certification principles applicable to all aircraft and specific requirement related to aircraft types. For instance, all aircraft are not equipped with flight envelope protections systems and need different attitude alerting/trigger thresholds.

But there is a fundamental difference between an on board protection or safety warning logic designed to avoid an accident, and a QR-FRD trigger designed to be activated only when an accident “will happen”.

Referring to the loss of control accident risk, the activation of a stall warning in flight does not mean that a loss of control accident will inevitably happen. This is one of several lines of defense in place to prevent catastrophic accidents.

The “perfect triggers” should activate only when all safety barriers having failed, including safety warnings presented to the pilots, an accident becomes inevitable.

The idea that QR-FRD triggers could be designed to be activated earlier than, and independently from on board safety warnings is questionable regarding legal aspects. If such credible triggers do exist, why not alerting the crew?

Certification authorities would have to justify the fact that these triggers are not required to be part of the cockpit alerting systems.

5.3 FB3 – Data Transport

The QR-FRD study has shown that among the different datalink service providers, the most serious candidates are:

- Satellite communications service providers as systems are already in place and currently used for cockpit and cabin services (QR-FRD D1 [Ref 1] section 3.2.5). Satellite communications have the most important coverage and use a protected aeronautical spectrum. To be noted, the future 5G mobile non-terrestrial network will rely on satellite communications.
- Terrestrial cellular network service providers (2G, 3G, 4G or 5G), but it will be limited to Base Station coverage (up to 30 km), and at ground or low-level altitude (under 1000 m) (QR-FRD D1 section 3.2.6) and does not rely on a protected aeronautical spectrum.

As the QR-FRD study particularly focuses on the recovery of data in remote locations, the data transport will most likely be assured by satellite communications and the terrestrial network will play a residual part, mostly when the aircraft is still ground-based.

As QR-FRD Study D4 [Ref 4] indicates, while in cruise, satellite communications will ensure data transport and cellular telephony will play a residual part mostly when the aircraft is still on the ground. For solution #1, "*As continuous transmissions are envisioned to start on the ground, continue in the air over oceanic and remote regions, and end on the ground, both cellular telephony and satellite communication media will be managed by the AIDS router and possibly the PIESD router"*. For solution #2, "*triggered transmissions are envisioned to occur when the aircraft is in the air, so only satellite communication media will be management by the AIDS router and possibly the PIESD router*" (p. 13/39).

5.3.1 Legal Framework

The legal framework applicable to satellite and cellular/mobile communications in the aeronautical field is built and based on the interactions of two UNO entities: the International Telecommunication Union (ITU) and the ICAO. The relevant EU regulations and directives will be mentioned. Certification and ISO Standards also play an important part. Finally, the issue of data protection when "traveling" in outer space will be addressed.

5.3.1.1 International Telecommunication Union and ICAO Standards and their interactions

One of the tasks the ICAO is to participate to the ITU Conferences and to obtain or maintain the allocation of protected frequencies for aeronautical purposes.

Indeed, the radio frequency spectrum is a limited natural resource and the ITU periodically reviews the allocation of frequencies during the World Radio Conferences.

In its 2019 Resolutions 222 and 426, the ITU insists on the fact that the use of spectrum must be guaranteed and invites the ICAO to evaluate what are the needs (Resolution 222) and the ITU will review if it is necessary to modify the ITU Regulations to reflect the new needs identified (Resolution 426). The next World Radio Conference is set to take place in November and December 2023.

The frequencies for satellite and mobile/cellular communications are not the same but they all rely on the allocation of frequencies by the ITU. Like the frequencies used for satellite communications, specific frequencies used by the cellular/mobile network are dedicated to aeronautical purposes.

Manual doc. 10054 on Location of Aircraft in Distress and Flight Data Recovery [Ref 15] also deals with data transport and points out that the timely recovery of flight recorder data allows to use "*any type of spectrum allocated on a primary basis to the function being performed*" and that however "*overall end-to-end reliability of recovering the flight recorder data is expected to not be worse than the reliability of the recovery of flight recorder data from a fixed flight recorder*" (section 3.6.10.10). The Manual insists on the fact that "*the availability of flight recorder data recovery services has to be considered when selecting the service provider used in the aera flown by the aeroplane*" (section 3.6.11.6).

The Manual allows the use of the PIESD as it states that "*it is acceptable to utilize commercial connectivity services to transmit flight recorder data*" (section 3.6.11.7) and that "If the

transmission of the flight recorder data is utilizing commercial connectivity services, the transmission of fight data required for compliance with the timely recovery of flight data and aircraft tracking mandates takes precedence over the non-required communication services data to keep the maximum bandwidth for the safety purposes. Non-required communication services provide flight crew and passengers with air-ground/air-air voice and data communication services" (section 3.6.10.10).

Finally, the ICAO has recently acknowledged the importance of cybersecurity, as "*the civil aviation sector is increasingly reliant on the availability of information and communications technology systems as well as on the integrity and confidentiality of data*". Issued in October 2019, the ICAO "Aviation Cybersecurity Strategy" [Ref 17] communication defined seven principles that should constitute pillars to build this strategy (international cooperation, governance, effective legislation and regulations, cybersecurity policy, information sharing, incident management and emergency planning, capacity building, training, and cybersecurity culture)[25].

5.3.1.2 European law

European law also insists on the need to protect key sectors from cyber-security threats.

Directive (EU) 2016/1148 [Ref 27] concerning measures for a high common level of security of network and information systems across the Union (NIS) aims to improve cybersecurity in a number of key sectors, including the aviation sector. Indeed, air operators can be qualified as "*operator of essential services*" within the meaning of the Directive. It implies that they have an obligation to implement appropriate and proportionate measures to prevent and minimize the impact of potential incidents affecting the networks security.

Regulation (EU) 2019/881 [Ref 25] also addresses cyber-security risks and provides for a European certification framework[26]. This framework is currently under development by the Stakeholder Cybersecurity Certification Group (SCCG). The purpose of this framework is to provide rules for protection against various cyberattacks according to the level of risk of the telecommunications installations concerned.

The security objectives to be achieved are the protection of data whatever their treatment (stored, transmitted or other) against accidental or unauthorized access or diffusion, and against accidental or unauthorized destruction, loss or alteration. Another objective is resiliency, which means restoring the availability of data, services and functions as well as access to them in a timely manner in the event of a physical or technical incident[27].

5.3.1.3 ISO Standards

The ISO standards dealing with information security are relevant for both FB3 and FB4 as they do not differentiate data transmission and data storage when it comes to data protection.

[25] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.
[26] Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[27] Article 51 of the Regulation (EU) 2019/881 of 17 April 2019.

Indeed, ISO 27001 (Information security management – Information technology) [Ref 32] and ISO 27002 (Information Technology – Security Techniques – Code of practice for information security controls) [Ref 33] are applicable to all business sectors dealing with data.

Concerning the organization and general management, the standards recommend that the roles and responsibilities of each party be defined contractually when an operator has recourse to a subcontractor (ISO 27002 section 15.2 on relations with service providers).

More specifically, on data transfer, section 13.1 of ISO 27001 states that "formal transfer policies, procedures and measures should be in place to protect the transfer of information over all types of communications equipment". This means that the process should be designed "to protect transferred information from interception, copying, modification, misrouting and destruction" and it is as an example recommended to use encryption techniques for the purpose of data protection.

5.3.1.4 Data protection in outer space

The 1967 international Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, better known as the Outer Space Treaty, has been drafted "*before the time of data*"[28] and does not address the use of space for data processing, nor the status of data in outer space or their protection.

As transnational data protection law has been described as a rather "*chaotic landscape*", a recent publication considers that "*the European GDPR has unleashed a wave of data protection legislation drafting around the world, mainly due to its extraterritorial application, which has notable legal implication for satellite operators*"[29].

The potential application of the GDPR [Ref 23] as the "gold standard" for data protection when a satellite is involved in its processing is discussed.

Some argue that there is a loophole in the GDPR. Its article 44 on "General Principle for transfers" refers to "countries" and "international organizations" and therefore only deals with transfers on Earth[30].

To the contrary, others consider that what needs to be looked at is who is the controller and the processer and "*whether they are subject to the GDPR and whether the satellites are under their control*": "*it is not because space objects are in space that the GDPR does not apply*"[31].

The present study is in favor of the second opinion. As clearly stated in an article, "*in the confusion regarding whether the provision on extraterritorial application of the GDPR will apply in case of communication and data transmissions via satellite, it can be said that, even though*

[28] Martin M. Zoltic and Jenny L. Colgate, « The Application of Data Protection Laws in (Outer) Space ». Available at: https://www.rothwellfigg.com/media/publication/15015_ICLG__Data_Protection_2019_RothwellFigg_Outer_Space.pdf
[29] Pedro R. Borges de Carvalho, « Transnational Space Law in the 21st Century: What laws govern data in outer space? ». Available at: https://tclf.in/2020/10/03/transnational-space-law-in-the-21st-century-what-laws-govern-data-in-outer-space/
[30] Martin M. Zoltic and Jenny L. Colgate, « The Application of Data Protection Laws in (Outer) Space »
[31] Magda Cocco and Helena Correia Mendonça, « GDPR for Satellite Operators: What you need to know », June 2018. Available at: https://interactive.satellitetoday.com/via/july-2018/gdpr-for-satellite-operators-what-you-need-to-know/

government satellites and remote sensing are involved, if personal data of EU citizens are concerned, and data is processed on the earth, the GDPR should apply"[32].

But, to avoid any dispute, article 22 of Regulation 996/2010 "*on access to documents and protection of personal data*" [Ref 20][Ref 20] could be amended to specify that the Regulation applies in accordance with the GDPR[33], the scope of which extends to data processing by any electronic communications networks, including satellite communications. Reference could be made to the definition of electronic communications networks in Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (article 2).

The definition is as follow:

> "*'electronic communications network' means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems*"[34].

This definition indeed confirms that no distinction is to be made in consideration of the type of electronic communications network.

5.3.2 Data transmission service providers (DTSP)

This section focuses on the satellite service providers, the main ground station networks providers and also potential and future other providers and aims to analyze their liability.

The study was meant to examine any risks of conflicts of interests or of duties in case the DTS provider could be the aircraft or engine manufacturer, an NAA or an ATM/ANS service provider. It has shown that such is not the case as neither of these actors will act as DTS providers[35].

5.3.2.1 Presentation of the main service providers

QR-FRD Study D2 [Ref 2] indicates that because of the ICAO North Atlantic Data Link Mandate, most aircraft are already equipped with antennas for satellite communications and use the services provided by Iridium, MTSAT and Inmarsat. Indeed, as the North Atlantic Airspace which links Europe and North America is the busiest oceanic airspace and that for the most part, direct controller-pilot communications and ATS surveillance are unavailable, the

[32] S. BU-Pasha and H. Kuusniemi, « Data Protection and space: What challenges will the General Data Protection Regulation face when dealing with space-based data? » *Journal of Data Protection and Privacy*, 2021, Vol. 4,1, 52-58. Available at: https://helda.helsinki.fi/bitstream/handle/10138/326365/Data_protection_and_space_Bu_Pasha_Shakila_and_Kuusniemi_Heidi.pdf?sequence=1

[33] Article 22 of Regulation 996/2010 refers to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the movement of such data. This Directive was repealed by article 94 of the GDPR, which indicates that « *References to the repealed Directive shall be construed as references to this Regulation* ».

[34] Directive 2016/1148 concerning measures for a high-level security of network and information systems across the Union directly refers to this definition in its article 4.

[35] The issue of conflicts of interests will be studied in depth in section 5.4.2 on recipients of the data.

North Atlantic Systems Planning Group[36] has concluded in 2012 the North Atlantic data link mandate to obligate operators to equip aircraft with enhanced air/ground communications tools (designated as FANS – Future Air Navigation Systems) and among them, satellite communications such as provided by Inmarsat and Iridium. The mandate has had full effect since February 2021[37].

So, regarding satellite communications, there are for now two main service providers, Inmarsat and Iridium, even though new service providers could be considered in the future (see Study D1 [Ref 1]).

Both Inmarsat and Iridium are private companies (Inmarsat was privatized in 1999). Inmarsat uses the geostationary orbit (GEO) while Iridium uses the low earth orbit (LEO).

It must be noted that the European Commission has introduced in February 2022 a proposal for a Regulation on an EU approach on Space Traffic Management. In other words, the EU wants to have a sovereign and public constellation to "*ensure the long-term availability of worldwide uninterrupted access to secure and cost-effective communication services. It will support the protection of critical infrastructures, surveillance, external actions, crisis management and applications that are critical for Member States' economy, security and defense*"[38]. The QR-FRD could be considered as an application that is critical for the Member States' economy and security. Nevertheless, this project, as it also focuses on the need to set out the appropriate normative and legislative framework and to establish international partnerships and engaging a multilateral level, could have an impact on the future QR-FRD system.

As suggested in QR-FRD Study D1 [Ref 1], other constellations, already in place or in development phase could be considered. The Starlink and OneWeb constellations, as they will supposedly offer wider bandwidth and higher data transmission speed, could be for instance potential candidates for the QR-FRD. Also, the technical capacity of present constellations to take over the QR-FRD has been questioned and will need to be further investigated.

All satellite constellations have ground stations to allow data communications, either their own or provided by a subcontractor (for instance, Amazon offers ground stations services).

Thus, the service providers to be considered for data transmission are:

- the Terrestrial mobile network providers;
- the satellite constellations and satellite communications providers (Iridium, Inmarsat);
- the ground station providers, when different from the satellite providers.

But data transmission via satellite communications also involve:

- the aircraft manufacturers as they team up with the satellite communication providers to install the antennas and tools on the aircraft;

[36] https://www.icao.int/EURNAT/Pages/EURNAT-Meetings-NATSPG.aspx: « *The North Atlantic Systems Planning Group (NAT SPG) was established in 1965 by the Council of ICAO the first regional planning group. From its Terms of Reference the NAT SPG shall continuously study, monitor and evaluate Air Navigation systems in the light of changing traffic characteristics, technological advances and updated traffic forecasts* ».

[37] See ICAO, North Atlantic Operations and Airspace Manual – NAT doc. 007, 2019

[38] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_921

- the airlines as aircraft operators.

5.3.2.2 Liability of the DTSP and solution proposals

The above description of the service providers highlights that the FB3 will mostly, if not only, rely on private actors.

Regarding satellite communications, the main service providers will probably have a contractual liability toward the aircraft operators (mainly airlines).

ISO certification appears to be a good way to ensure the protection of the transmitted data "from interception, copying, modification, misrouting and destruction" (ISO 27001:2017 section 13.1 [Ref 32]).

5.3.3 Cases study

The Malaysia Airlines MH370 case highlights different issues at the FB3 / data transfer stage.

We do not know what happened on board of the Malaysian aircraft on 07 March 2014, after the last routine communication with Kuala Lumpur ACC, but it seems reasonable to say that any data transmission capacity would have been lost the same way as other communications means[39]. A sudden major failure or an intentional disconnection of all transmission systems have to be envisaged.

Regarding the latter, no operational procedure leads to such an action which should be considered as an unlawful interference out of the scope of the present QR-FRD study. However, the ICAO Annex 13 [Ref 8] accident definitions include the disappearance of an aircraft and with or without aircraft disappearance, any suspected unlawful interferences should not refrain AIAs from, at a minimum, understand "in a timely manner" the nature of the occurrence.

Whatever the MH370 accident causes were, it is probable that any different outcome regarding the communication loss would have required significant changes in the equipment design to make data communication systems more robust in case of system failure or to make them impossible to be disconnected intentionally. This should apply to the QR-FRD too as a communication system and pleads in favour of new certification requirements for on-board transmission equipments regarding these two aspects.

When considering the Air France AF447 accident case used previously (FB2 aspects) and the MH370 accident we may observe that both triggered and continuous solutions would involve similar data transport segments.

Had these flight been equipped with QR-FRD systems, data transport would have probably involved different service provider contractual aspects and legal environments.

Because of its destination (Beijing) and because of the presence on board of a significant number of Chinese citizens, the Malaysian flight accident illustrates some specificities of Chinese law regarding data transport.

[39] Except for the hourly periodic « hand-shakes » with the Inmarsat satellite.

These aspects will be examined in the § 5.4 FB4 – Off-aircraft storage

Unlawful interferences are not in the cope of this study. However, in addition to the possibility of a multiple transmission system failures on board of the flight MH370, an intentional systems disconnection by somebody on board must be envisaged. This should encourage the implementation of an independent and as autonomous as possible transmission system.

The possibility of intercepting the transmission must be envisaged.

Service providers must demonstrate QR-FRD system robustness regarding these threats.

5.4 FB4 – Off-aircraft storage

For Off-Aircraft storage, the main issues are to guarantee the protection of the data by all the different recipients and ensure that the relevant AIAs will have access to the data "*in a timely manner*".

The main actors at this stage are the airlines and the data centers but this chapter will explore the possibility of central repository in charge of the FRD storage.

5.4.1 Legal Framework

5.4.1.1 ICAO Standards

The main relevant ICAO Standards are Annexes 6[Ref 6], 13 [Ref 8] and 19 [Ref 9]. Furthermore, Part II of the ICAO Manual doc. 10054 [Ref 15] contains important recommendations on the practical implementation of the protection.

First, it is important to note that, depending on the outcome of the event that triggered the transmission of the data, the protection regime that applies may differ.

Either no accident or incident subject to an official safety investigation occurs and the protection of Annex 19 applies: This is the case when the data transmission is continuous because not all the data collected at these times will be used for investigation purposes. In most cases, these data will not be transmitted to the AIAs[40]. This is also the case when the event triggering the transmission will reveal to be a "false-positive".

Or an accident or serious incident occurs: both Annexes 19 and 13 will apply.

ICAO standards address the transmission of flight data from the aircraft after an accident. In this context, many recommendations are relevant to us because they deal with the reception of the data by the operator before their transmission to the competent AIA.

ICAO Manual 10054 states that "*after an accident, the State of the Operator of the aircraft involved should comply with the procedure for ensuring the safe custody of the data until the latter are delivered to the AIA of the State of Occurrence. The procedure should ensure protection and integrity during the transfer of data to the AIA of the State of Occurrence or to the AIA of the State conducting the accident or incident investigation*" (section 3.6.3.3). If it

[40] It has been suggested that this data could, once anonymized, be collected by airlines as part of their safety management system. This question however falls out of the scope of this study.

deals with data transfer, it also covers data storage as the data must be protected throughout the whole process, until it is transferred to the competent AIA.

The Manual mentions the responsibility of operators regarding the external data transmission services that they may decide to use. In particular, the operator "*is expected to carefully consider the guarantees offered by such services before subscribing to them*" (section 3.3.6.4 and 3.6.2.2). In any case, the operators "*remain fully responsible for protecting these data against unauthorized access and for providing unaltered and unprocessed data to the appropriate authorities*" (section 3.6.2.1).

Regarding data storage, Annex 6 provides that: "*the operator shall ensure, to the extent possible, in the event the aeroplane becomes involved in an accident or incident, the preservation of all related flight recorder records and, if necessary, the associated flight recorders, and their retention in safe custody pending their disposition as determined in accordance with Annex 13*" (Part I, section 11.6).

5.4.1.2 GDPR

As mentioned above, this regulation is only applicable to personal data. It has an important place in our study because it has a broad scope of application (section 4.1.2).

Under the GDPR [Ref 23], airlines are data controllers, meaning a "*natural or legal person who determines the purposes and means of the processing of personal data*" (article 4(7)). When they use subcontractors (data storage centers) to store the recovered data, then the latters are described as data processors, meaning "*a natural or legal person which processes personal data on behalf of the controller*" (article 4(8))[41].

First, the GDPR provides several obligations for the data controller. It has to "*implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation*" (article 24(1)).

When the airline uses a subcontractor to store recovered data, then it must verify that the subcontractor provides sufficient guarantees to ensure its ability to maintain the confidentiality, integrity, availability and resilience of the data (article 28(1)).

Secondly, according to article 28, the GDPR also provides obligations for the data processor. They are first bound by the same obligations as the data controller Moreover, they cannot engage another processor – and other subcontractor - "*without prior specific or general written authorization of the controller*" and they can process the personal data "*only on documented instructions from the controller".* When the processing is completed, they have to "*delete or return all the personal data to the controller*". Finally, they make "*available to the controller all information necessary to demonstrate compliance with*" these obligations which must be set out in a written contract.

As data centres could be in a country other than an EU member state, the GDPR has made provisions for this hypothesis. Article 44 of GDPR ensures that the operator will transfer the data only to entities offering sufficient guarantees and GDPR compatible. To that effect, the

[41] Where the purposes and means of the processing of data are determined by law – as could be the case if a QR-FRD process was made mandatory – the law may designate the controller (GDPR article 4(7)). This provision could be used to prevent conflicts of interest (see 5.4.2.3.3 below).

EU Commission has put in place tools to assess the level of protection offered by the service provider's local regulations and some countries are subject to adequacy decisions[42].

When it cannot be sure that local regulations are GDPR compliant, additional guarantees from the service providers are needed.

The EU relies on several tools to ensure the application of these guarantees (article 46 of the GDPR):

- Corporate Binding Rules: foreign companies may provide for binding rules that must be approved by the competent supervisory authority;
- Code of Conduct and Certification Mechanism: Certification and adherence to a code of conduct are considered a way to comply with the provisions of the GDPR.
- Standard contractual clauses: the European Commission has published standard contractual clauses to be inserted in contracts between the importer and the receiver of data. These clauses are a good way to comply with the GDPR.

The 16 July 2020 ECJ "Schrems II" decision [Ref 29] called into question such clauses, as, in certain situations, they may not constitute per se a sufficient safeguard to ensure the effective protection of personal data transferred[43]. In particular, they are not sufficient if the local law allows public authorities to interfere with the rights of individuals. In this decision, the Court judges that because US law allows such interference[44], standard contractual clauses do not constitute a sufficient guarantee for data transfer to the United States.

As a result of this decision, the standard contractual clauses have been revised and a section II entitled "*Local Laws and Obligations in the Event of Access by Public Authorities*" has been added[45]. The clauses now provide that the parties agree to conduct an analysis of local law and its concrete application to the data concerned. In the event of a proven risk, additional clauses may be stipulated providing for additional obligations for the party receiving the data (including the obligation to notify the data controller when the public authorities make a request for data, the obligation to use existing remedies, the obligation to minimize the data transmitted to the authorities).

The European Data Protection Board [Ref 31] has also published recommendations to help companies analyze local rights and outline possible additional measures to protect data[46].

The possibility of transferring data to a third country by means of standard contractual clauses has therefore been reduced, but it remains possible provided that local considerations are taken into account.

[42] The European Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.

[43] Judgment of the Court (Grand Chamber) of 16 July 2020, "Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems", No. C-311/18, ECLI:EU:C:2020:559

[44] Section 702 of the Foreign Intelligence Surveillance Act allows the National Security Agency to collect data collect certain data from U.S. companies, for intelligence purposes and outside of any legal proceedings.

[45] Commission implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[46] EDPB, Recommendations 01/2020 on measures to complement transfer instruments to ensure compliance with the EU level of personal data protection of 18 June 2021

These various provisions are binding and imply the implementation of an effective guarantee mechanism even in countries not GDPR compliant.

Finally, article 49 of the GDPR [Ref 23] provides for an exception: "*In the absence of an adequacy decision pursuant to Article 45, or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only (…) if the transfer is necessary for important reasons of public interest*".

This exception may be interesting in our case because the QR-FRD appears as a technology implemented in the public interest. Moreover, Recital 112 of the GDPR states that such a derogation is lawful "*where it is necessary to protect an interest which is essential for the data subject's or another person's vital interest, including physical integrity or life (…)*".

Recital 112 gives examples of "*important reasons of public interests*" such as "*international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport*". There is no doubt that the prevention of accidents and serious incidents would fit in that list of examples.

The European Data Protection Board [Ref 30] has issued guidelines on the application of Article 49 on derogations in the context of transfers of personal data to third countries[47]. If matters of aeronautical safety fall within the scope of that derogation, the problem for QR-FRD is that the Board considers that even though data transfers for reasons of public interest are not required to be "occasional", "*this does not mean that data transfers on the basis of the important public interest derogation can take place on a large scale in a systematic manner*" as they should not become "the rule" in practice. This interpretation could largely limit the possibility to invoke the article 49 exception on a regular basis as QR-FRD could be seen as a "*large scale and systematic*" system: the compliance of third countries to the GDPR or equivalent data protection schemes is therefore necessary for a full and complete implementation of QR-FRD.

5.4.1.3 ISO Standards

ISO certification is a way to comply with the GDPR. Indeed, the regulation repeatedly encourages controllers and processors to use certification to demonstrate their compliance with it[48].

5.4.1.3.1 Standards for the protection of data

A series of standards provides rules concerning "information safety. These standards are ISO 27000, ISO 27001 [Ref 32], ISO 27002 [Ref 33], ISO 27701 [Ref 34][Ref 34], ISO 27018 [Ref 35] and ISO 27040 [Ref 36].

ISO 27001 and ISO 27002 standards defines the guiding principles of information safety, applicable to all business sectors dealing with data.

[47] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Adopted on 25 May 2018.
[48] GDPR, Articles 24 3., 28 5. 6., 32 3., 42.

The ISO 27701 standard is an extension of the two previous standards. It specifies how each principle applies in the particular case of personal data and adds recommendations when it deems necessary. Appendix D is particularly interesting because it explains how compliance with the requirements and measures of this document can be relevant to meeting the requirements of the GDPR. For this purpose, a table of correspondences between ISO standards and the regulation is established.

This standard notably adds recommendations to the previous standards regarding the data subject's right to enable certified companies to fully comply with the GDPR. In this instance, Section 7 introduces new obligations for data controllers whereas Section 8 provides additional ones for data processors.

Concerning the data controller:

GDPR	ISO 27701
Article 5 - Principles relating to processing of personal data: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability	**7.2.1**: obligation to identify and document the specific purposes for which the personal data will be processed. **7.2.5**: obligation to conduct a privacy impact analysis whenever a new processing of personal data is planned **7.4.1**: obligation to limit collection to the minimum that is relevant, proportionate and necessary for the purposes identified **7.4.2**: obligation to limit the treatment under the same conditions **7.4.4**: obligation to define and document minimisation targets and define the methods for achieving them **7.4.5**: obligation to delete data at the end of processing or to make it impossible to identify or re-identify data subjects **7.4.7**: obligation to keep data only for the time necessary for processing
Article 6 - Lawfulness of processing **Article 7, 8** – Conditions for consent	**7.2.2**: obligation to comply with the relevant legal basis for processing personal data, including obtaining the subject's consent where necessary. **7.3.4**: obligation to provide a mechanism to change or revoke consent
Article 12, 13, 14 – Information of data subjects	**7.3.3**: obligation to determine the information to be provided to data subjects **7.3.3**: obligation to provide this information
Article 15 – Right to access by the data subject	**7.3.6**: obligation to organise a right of access to data
Article 16 – Right to rectification	**7.3.6**: obligation to organise a right of rectification of data
Article 17 – Right to erasure / right to be forgotten	**7.3.6**: obligation to organise a right of erasure of data

GDPR	ISO 27701
Article 18 – Right to restriction of processing	**7.4.1**: obligation to limit collection to the minimum that is relevant, proportionate, and necessary for the purposes identified **7.4.2**: obligation to limit the treatment under the same conditions
Article 21 – Right to object	**7.3.5**: obligation to provide a right to object to the processing of personal data

For the data processor, paragraphs 8.2.1 and 8.2.2 of Standard 27701 provide an obligation to respect the purposes of the processing as established in the contract concluded with the data controller.

These provisions are relevant if no accident occurs, as in this scenario the rights of data subjects cannot suffer any exception and must be guaranteed (see Section 5.1.2).

The ISO 27018 standard is sector specific. It specifies the requirements of the ISO 27002 standard for data centers. Annex A of the standard is interesting because it provides additional protection measures: obligation to comply with the controller's instructions; obligation to erase or destroy data after processing; obligation to inform the controller of any lawful request for disclosure of personal data from a law enforcement authority unless such disclosure is prohibited; obligation to inform when unauthorized access to facilities and data has resulted in loss, alteration or disclosure of data; provide a policy for the return, transfer or deletion of personal data; confidentiality obligation involving all agents, which must survive the contract; obligation to restrict the creation of paper media containing personal data; encrypt data; authorization required before transferring personal data; personal access code for authorized employees; the subcontractor specifies and documents the countries in which personal data can potentially be stored, etc.

Finally, the ISO 27040 standard is specific to the storage activity. It provides guidance for the safety of data storage.

5.4.1.3.2 Standards for the protection of data storage infrastructures

A second set of ISO standards concerns the physical protection of data centers and access restriction.

A first standard was created at European level: EN 50600-x-y [Ref 38]. Then, an ISO standard replaced it, taking over the European standard in its entirety while adding an additional chapter "management and operational information". This is the ISO 22237 package[Ref 37]. It deals with building construction, energy supply and distribution, environmental control, dedicated cabling infrastructure telecommunications, security system and earthquake risk. ISO 27002 also provides several recommendations to the physical protection of data centers.

All these standards are interesting because they are already known by the aeronautics industry and are international references.

5.4.2 Recipients of flight recorder data

Flight Recorder Data are recorded for the purpose of accident investigations. The final data recipients will therefore be AIAs. However, given that the competent AIA is impossible to identify before an accident has occurred[49], it cannot be chosen as the initial recipient in charge of storing the data.

The responsibility to store the data must be vested in another entity so that once identified, the competent AIA can have access to it in a timely manner.

This raises issues of conflicts of interests because most stakeholders have an interest in the investigations' findings (5.4.2.1). This section will therefore explore the option of entrusting the data to one of the existing actors in the field (5.4.2.2) or to resort to other options to avoid any risk of conflicts of interest (5.4.2.3).

5.4.2.1 Storing the data can expose the data controller to suspicions

In France, the investigation that followed the 26 June 1988 A320 crash of Habsheim provides an example of how perception can undermine the public's confidence in the accident investigation system set up under Annex 13 [Ref 8]. Both safety recorders (CVR and FDR) were taken from the accident site and flown to the AIA's laboratory with no specific precautions or judicial supervision. During the criminal investigation that followed, the pilot challenged the recordings' authenticity and the AIA's conclusions.

Books and articles were published, accusing the ministry of transport, the French AIA, the French CAA and the aircraft manufacturer of tampering with the recordings in order to dissimulate flaws of the aircraft itself. It took a decade, until the trial and the appeal took place in 1997 and 1998 respectively, before the criminal courts confirmed the recordings' authenticity and the AIA's initial conclusions. In the meantime, trust in the system was durably affected.

This shows that the public perception that a conflict **might** exist is just as problematic as if the conflict actually did exist. For example, ICAO gives the following definition of conflicts of interest:

"*A situation in which an official has private interests that may, **or be perceived to**, improperly influence or interfere with the performance of official duties and responsibilities*" [50] (emphasis added).

Similarly, French law gives the following definition:

"*A situation of interference between a public interest and private or public interests that is likely to influence **or appear to** influence the independent, impartial and objective exercise of a function*"[51] (emphasis added).

[49] In particular, it can generally not be assumed that the same AIA will always be competent to investigate one given operator's accidents or incidents, unless that operator operates exclusively in only one country.
[50] ICAO, *Conflict of interest in civil aviation* (July 2019)
http://www.icscc.org.cn/upload/file/20201009/20201009101625_28249.pdf
[51] Law of 11 October 2013 promoting transparency of public life.

When determining who should have control of the data while it is stored, specific attention should therefore be given to the issue of conflict of interests and solutions should be sought to avoid them.

5.4.2.2 Existing actors in the field

This section will examine whether existing actors in the field under study could be chosen to take the responsibility of storing the Flight Recorder Data and guarantee its integrity until it can be recovered by the competent AIA.

Airlines, manufacturers, ATM/ANSPs, CAAs will be assessed but they all have in common that depending on the circumstances of the accident, they may have a stake in the outcome of the investigation.

This creates a situation where their private interest can *be perceived* (by the general public) *to improperly influence or interfere with the performance of their official responsibility* to guarantee the data's integrity – which is the very definition of a conflict of interests.

5.4.2.2.1 Airlines

Airline operators are the first obvious option. They will be the actors in charge of implementing the QR-FRD system and some of them already collect data sent from their aircraft for other purposes such as maintenance or their SMS. They could be encouraged to bear the related costs by the fact that (depending on the adopted configuration) some of the data collected through the QR-FRD system can be used as an additional and efficient means to feed their SMS[52].

The disadvantage of this solution is that it would put airlines in a conflict-of-interest situation (see section 5.4.2.2.). Indeed, it would give them control over data that they would hold for no purpose other than the investigation, while at the same time having an interest in the outcome of that investigation. This conflict between their private interest and their public obligations could appear, rightly or wrongly, to influence the way they discharge their duties and give rise to suspicions.

Another disadvantage of this situation is that each airline is likely to have its own data storage policy and the data storage will also be affected by the data centers' service providers' policies. Frequent and usual for data storage, the possibility of multiple data copies being stored in multiple locations could also have an impact on the applicable law.

If airlines were chosen as recipients of the FRD, precise and specific standards should therefore be elaborated to address the conflict of interest that this option would create and to regulate the storage of that data-by-data centers (see section 5.4.1.3.1).

5.4.2.2.2 Aircraft or engine manufacturers

[52] This question has not been further examined because it falls out of the scope of the present study, which is limited to the QR-FRD process.

Aircraft and engine manufacturers are in a similar situation: they already receive some data from the aircraft so it could seem natural to consider them for this new mission.

However, this new mission would require that they receive much larger amounts of data, most of which will have little or no relation to their own activity and expertise. There is no natural reason for them to do so. The costs required to fulfil such a mission would not be covered by their normal income unless they could invoice them to AIAs or airlines, but airlines might be reluctant to provide manufacturers freely with valuable recorded data that they have paid for (data recorders, flight operations, data process)

And in addition, manufacturers also may have an interest in the outcome of the investigation, which means that their situation in terms of conflict of interests would not be better than that of airlines.

5.4.2.2.3 ATM/ANSPs

Entities involved in Air Traffic Management (ATM) or Air Navigation Service Providers (ANSPs) present the same characteristics: they too already receive some data from the aircraft so it could seem logical to investigate the possibility of asking them to store the FRD until it can be turned over to the competent AIA.

However, the drawbacks identified for manufacturers apply here in the same way: it is not their mission to store data largely unrelated to their field of activity and expertise; the issue of funding this activity raises the same questions; and they too can be seen to have a conflict of interests as ANSPs may have a responsibility in some accidents or incidents, and thus an interest in the outcome of the investigation.

5.4.2.2.4 Civil aviation authorities

Given the strong public interest in ensuring the data's authenticity and integrity, the choice could be made to consider that only a public authority should be the intended FRD recipient. The most obvious candidates for such a mission would be civil aviation authorities, whether national or European, in the case of EASA. EASA for instance already manages the European Co-ordination Center for Accident and Incident Reporting Systems (ECCAIRS) platform.

But in addition to the fact that all civil aviation authorities may not easily find the resources necessary for an additional mission, this would place them in the same conflict-of-interest situation as airlines, manufacturers or ANSPs given that they too may have an interest in the outcome of accident investigations – a situation which could, rightly or wrongly, give rise to suspicions.

It therefore appears that by construction, vesting the responsibility to store the FRD in one of the actors in the field will almost inevitably create a conflict of interests. Solutions can be found to manage this situation, and some will be proposed below (see section 5.4.2.2), but it is worth examining other options that would allow to avoid the risk altogether, because they do not depend on actors involved in the processes that lead to the accident.

5.4.2.3 In search for a solution that would not rely on one of the actors in the field

This section will examine solutions that would not rely on entrusting the data to any of the involved actors.

For the sake of completeness, thought was given to the idea of resorting to the blockchain technology, which was ruled out. The option of resorting to a third party and possibly a "central repository" was then considered.

5.4.2.3.1 The use of blockchains does not seem relevant

Blockchain is a technique for storing and transmitting information with no central authority. A series of records, called blocks, are linked in a secure way, each containing the cryptographic hash of the previous block, a timestamp, and data. The data's inviolability is guaranteed by the fact that the inscription of a new block requires the agreement of the majority of the participants in the blockchain and that everyone has an up-to-date copy.

Blockchains were initially developed around cryptocurrencies: such blockchains are public, all participants having access to the registered data and being able to add blocks. This technology may appear attractive as a storage solution guaranteeing the integrity of data, however for the purposes of the QR-FRD project, it appears to be inappropriate for both technical and legal reasons.

Technically, it is impossible to transmit a large amount of data through the blockchain in a very short time. Blocks can only contain a very small amount of data (640 bits per transaction; by comparison a single tweet can hold up to around 2650 bits[53]). The blockchain technology is adapted to record transactions which require a small amount of information, but not to transmit the required amount of flight data in a restricted time.

The legal drawbacks are also dissuasive:

- blockchains are normally public, while the FRD should be kept confidential. It is possible to create private blockchains, restricted to a limited number of participants with modular rights to reading and inscription but this requires an intermediary within the blockchain to establish these modular rights, so that resorting to this technique loses some of its relevance;
- the requirement to encrypt the data also makes it less relevant to resort to the blockchain technique which was designed so that all participants could verify the data;
- FRD includes personal data that cannot be segregated from non-personal data, so that personal data protection rules, including the GDPR, must be respected. Making a blockchain GDPR compatible raises some difficulties, for instance:
- the GDPR implies defining the role of each party and contractualizing the relationships. Since in a blockchain everyone intervenes to endorse an entry, contractual relationships should be multiplied[54];
- the GDPR requires that data be minimized and deleted after processing, whereas the blockchain technology is meant to make it impossible to delete or modify data;

[53] Open Data Institute, "*Applying blockchain technology in global data infrastructure*", ODI-TR-2016-001, p. 20.
[54] See 5.4.2.2.2.

- the blockchain implies that all participants have a copy of the register: in addition to being energy-consuming and environmentally unfriendly, the dissemination of copies is contrary to the principle of data minimization provided by the GDPR.

Most of these legal drawbacks could be resolved (the blockchain could be private, participants' access to the data could be restricted etc…) but the blockchain technology would be distorted, to the point that the interest of resorting to it would become questionable.

5.4.2.3.2 Resorting to a third party would be the most efficient way of avoiding a conflict-of-interest situation

In the private sector, manufacturers, or sellers of the future QR-FRD system could find an interest in offering the additional service of storing the data and conveying it to the relevant AIAs when required to do so. Airlines could also resort to existing data storage providers.

This raises the question of who would finance this activity by buying such services.

The requirement to have a QR-FRD system being an operational rule (it is in Annex 6 and would logically be transposed in the EU air operation rules) the costs would logically be borne by operators. As mentioned in 5.4.2.1.1, the benefit of having an efficient mean to collect recorded data in near real time for their programs could be an incentive for such an investment[55].

It should be important that paying for this service does not give the airlines control over the data. Regulations and contracts should prohibit airline interference or involvement with data from an accident or serious incident under investigation, while precise standards for the storage and handling of such highly sensitive data would need to be adopted and imposed on the data centers (see section 5.4.1.3.1).

Public funding could however be another option given that aviation safety is a matter of public interest. Public bodies that could have a legitimate purpose in funding data centers for storing flight data could include governments (departments of transport), investigation authorities, civil aviation authorities…

This would obviously raise the same financial issues as those previously mentioned (all public entities will not easily find the necessary resources) but it would also largely reduce the appearance of conflicts of interests.

Public funding would also probably lead to consider the option of setting up one or a few dedicated repositories where all Flight Recorder Data would be stored, rather than letting each operator make its own choices.

5.4.2.3.3 A dedicated central repository?

One could imagine setting up a dedicated central repository, or a limited number of repositories from which airlines would have to choose. Limiting the number of storage service providers to just one or a few would undoubtedly foster numerous advantages, such as:

- better control of confidentiality;

[55] Although, as previsously mentioned, this option has not been examined here as it is not within the scope of this study.

- better assurance of compliance with all relevant regulations and standards;
- avoidance of conflicts of interests;
- easier mutual knowledge, understanding and trust between AIAs and the data repository.

The entity in charge of the repository would act as data storage service provider but should also take the full responsibility of acting as data controller, so that none of the entities interested in the investigation's outcome can appear to control the data. As mentioned above, the data controller can be designated by law (GDPR, article 4(7)). If the regulations implementing the QR-FRD process opted for a central repository, its designation as data controller until the AIA takes this responsibility over would resolve the airline's conflict of interests.

Such repository (or repositories) should be set up under the auspices of a neutral institution, whether already existing or to be created (AIAs could assemble together to create such a body; another option would be to guarantee that body's neutrality by organizing its governance with the involvement of all actors of the field, thereby neutralizing each other).

The main drawback is that airlines could be reluctant to waive the option of organizing their QR-FRD systems as they wish, unless the use of such dedicated repositories became mandatory or unless they found an interest in doing so, such as lower or no storage costs. This of course symmetrically again raises the difficulty for public entities to find the necessary resources.

5.4.2.4 Conclusions on the liability of the FRD recipient and solution proposals

The advantages and drawbacks of each above discussed solution can be summarized as follow:

	Advantages	Drawbacks
Airlines	• They already collect recorded data for other purposes (SMS, maintenance) • Some QR-FRD data could be used for their SMS. • Could be encouraged to bear the costs	• Conflict-of-interests, perceived or real (interest in the outcome of the investigations) • Multiple airlines = multiple data policies • Need to regulate their own service providers (data centres)
Aircraft or engine manufacturers	• They already collect data	• They would receive large amounts of data unrelated to their own activities • Conflict-of-interests, perceived or real (interest in the outcome of the investigations) • Airlines may be opposed to provide manufacturers freely with valuable recorded data they have paid for (data recorders, flight operations, data process)
ATM/ANSPs	• They already collect data	• They would receive large amounts of data unrelated to their own activities • Conflict-of-interests, perceived or real (interest in the outcome of the investigations)

	Advantages	Drawbacks
Civil aviation authorities	• Public confidence in the data's authenticity and integrity • Possible candidates like EASA already manages the ECCAIRS platform	• Funding • Conflict-of-interests, perceived or real (interest in the outcome of the investigations)
Blockchain	• Avoiding conflict-of-interests • No central authority • Ensuring inviolability and authenticity	• Technically impossible to transmit large amount of data in a very short time • Confidential logic of QR-FRD against the public logic of blockchain • Blockchain might not be GDPR compliant • Energy consuming
QR-FRD providers offering a storage service	• Avoiding conflict-of-interests	• Funding: private (airlines, manufacturers) or public (financial issues)
Dedicated central repository	• Avoiding conflict-of-interests • Better control of confidentiality • Better assurance of compliance with all relevant regulations and standards • Easier mutual knowledge, understanding and trust between AIAs and the data repository	• Airlines could be reluctant to waive the option of organizing the QR-FRD as they wish • Funding

It would go beyond this study's purposes to make a choice between the options that were reviewed in sections 5.4.2.1 and 5.4.2.2. Each of them raises legal, ethical, and economic issues that call for policy decisions.

- Whichever choice is made, the chosen data controller will be responsible for dealing with the data storage service provider and act as its "ordering customer". If its own interests become conflictual with those of the investigation, there is a risk that that data controller will appear likely to interfere with the data. To avoid or mitigate that risk, the following solutions have been identified: this potential conflict of interests is largely reduced when the data is encrypted and signed in the aircraft buffer, making data tampering very difficult, if not impossible[56];

- it should be ensured that the data never transits through the entity chosen to act as data controller but is sent from the aircraft directly to the storage center; if the chosen entity is the airline operator, and if it is decided to grant the airline access to the data for its own SMS purposes, then regulations should be adopted to ensure that it only receives a copy of the technical data but without any access to the original files, so that it cannot be suspect of tampering them;

- the repository itself should have a strong and solid status; the ideal solution would be to have one or a few dedicated central repositories supervised by a third party with no interest in the outcome of investigations.

In any case, Flight Recorder Data must be stored in data centers that will have to comply with the ISO standards examined in section 5.4.1.3, which are the strongest tool to ensure the

[56] See 5.1.3.

protection of the stored data by treating it all as if it were personal data, in compliance with GDPR rules.

ISO certification is one way to guarantee GDPR compliance[57]. ISO standards are international and likely to be accepted by all stakeholders, and they deal with both the protection of data as such, and the protection of the infrastructures hosting the data.

It is therefore recommended to integrate in ICAO Annex 6 [Ref 6] and in Manual 10054 [Ref 15] the following requirements:

- that the entities chosen to receive the data become certified to ISO 27000, 27001 [Ref 32], 27002 [Ref 33], 27018 [Ref 35], 27040 [Ref 36] and the ISO 22237 package [Ref 37] before they implement the QR-FRD system
- that they only contract with data centers that hold the same ISO certifications
- that contracts with the data centers specify the protections and responsibilities of each party; recommended contractual clauses can be inspired by the standard contractual clauses published by the European Commission[58]. They should also deal with issues specific to QR-FRD.

It should also be discussed whether States of data storage should be required to ensure that data recipients are subject to effective procedures and policies that guarantee the protection of the stored data[59]

5.4.3 Length of data retention and data deletion

Currently, flight recorders' data are not systematically extracted[60]. Flight recorders have a limited recording capacity. With each flight, the new data collected will overwrite and replace the old data. Annex 6 stipulates that at least the last 25 hours of CVR and FDR data must be kept[61] but in most cases, CVR and FDR data are deleted within a few days of being recorded.

The main difficulty with the QR-FRD is that data will be transmitted to a data storage provider. The storage capacities in the case of QR-FRD are virtually infinite, these data will not be replaced by new ones as is the case with the current recorders. It is therefore imperative to define a retention and deletion policy for QR-FRD data.

The ICAO standards limit the use of collected flight data in case of accident (Annex 13 5.12 [Ref 8]) or in the absence of accident (Annex 6 [Ref 6]) but do not provide for a maximum data retention period or for a data deletion policy.

Therefore, reference must be made to European Union law. The principle of data minimization provided by the GDPR must guide our reflections on this topic. According to it, personal data collected must be adequate, relevant and limited to what is necessary for the purposes for

[57] *Ibid*. ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.
[58] *Ibid*. Commission implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
[59] See ECJ 16 July 2020 decision [Ref 29].
[60] Exception: Recorded flight data are systematically extracted by airlines from Quick Access Recorder (QAR) equipment as part of their SMS/FDM programs.
[61] Annex 6, 6.3.1.3 concerning the FDR; Annex 6, 6.3.2.3.1 concerning the CVR.

which they are processed (Article 5). Thus, data must be deleted once their processing is no longer necessary.

Regulation (EU) No. 965/2012 of 5 October 2012 [Ref 21] provides: " *Following an accident, a serious incident or an occurrence identified by the investigating authority,* ***the operator of an aircraft shall preserve the original recorded data of the flight recorders for a period of 60 days or until otherwise directed by the investigating authority.***"[62].

This rule can be reused for the QR-FRD purposes. Indeed, in the event of an accident and transmission of data, the data storage provider could be required to retain the data for 60 days[63] and then be required to delete it.

In this context, a different formulation should be adopted: instead of making it an obligation to keep the data for a minimum period of time, an obligation to delete the data after 60 days should be introduced if not claimed by an AIA or if no accident occurs.

This obligation can result from a regulation which puts the airlines in charge of this delay, and which obliges them to include the same obligation in their contractual relationship with the data storage provider intervening in the chain of transmission of the QR-FRD. Thus, in the event of an accident or serious incident, the data service provider shall transmit the QR-FRD data to the competent AIA without keeping a copy. If no accident or serious incident occurs, the data service provider shall delete the data and these copies after 60 days.

5.5 FB6 – Data Recovery

This last functional block mainly concerns the AIAs as they are the final recipients of the data.

One significant evolution is that for QR-FRD, one AIA could have jurisdiction on the physical records and another on the data transmitted and stored in application of the QR-FRD.

This section will address the need to prevent data withholding by the State of data storage.

5.5.1 Determining the competent AIA

Existing rules of competence, as set out in sections 5.1 to 5.3 of Annex 13 [Ref 8] and very briefly summarized below, have no reason to be amended:

- in most circumstances, the State of Occurrence's AIA will be responsible for the investigation;
- if the State of Occurrence is not a party to the ICAO Convention or does not intend to initiate the investigation, it should then be conducted by the State of Registry, or failing that, by the State of the Operator, the State of Design or the State of the Manufacturer;
- similarly, if the accident takes place outside the territory of any State (for instance over the ocean) or if its location is unknown, the State of Registry's AIA will be responsible for the

[62] CAT.GEN.MPA.195.
[63] This delay is an indication but can be renegotiated between stakeholders of the QR-FRD as long as the principle of data minimization provided by the GDPR is respected.

investigation, or failing that, the State of the Operator, the State of Design or the State of the Manufacturer.

Under these rules only one single AIA can be competent to carry out the investigation (even though Annex 13 does encourage giving the investigation an international nature by providing for the participation of accredited representatives from other States) and that single AIA will normally be the one of the State where the accident occurred, with the easiest access to the accident site, the wreckage and the flight recorders[64].

The fact that in the future, the flight records may be obtained without access to the wreckage does not mean that the State of Occurrence's AIA should be replaced by another one: as already mentioned, access to the accident site, the wreckage, the witnesses, means that the State of Occurrence's AIA will remain the best placed to conduct the investigations.

The State of Storage has no particular interest in the accident just because the data was stored on its territory. It is already possible to seek its assistance under the rules of Annex 13 that provide that "*any State shall, on request from the State conducting the investigation (…) provide that State with all the relevant information available to it*" (section 5.14).

ICAO's Accident Investigation Panel has already proposed to supplement this rule by adding the following provisions as a new section 5.14.2:

"If a State has available to it any data from a flight recorder of an aircraft involved in an accident or incident, that State:

a) shall, without delay, provide the State conducting the investigation with all such data available to them; and

b) shall not divulge such data without the express consent of the State conducting the investigation" [65].

Introducing such wording would be appropriate indeed, even though Annex 13 already addresses a somewhat similar situation where the State of Occurrence's AIA does not have direct access to the recorders, because the aircraft was able to land in another State: section 5.16 then puts the onus on the State of Registry or State of the Operator to "*furnish the [State conducting the investigation] with the flight recorder records and, if necessary, the associated flight recorders*".

The combination of this existing rule 5.16 and the proposed rule 5.14.2 would mean that the State of Registry, the State of the Operator and the State on whose territory the data is stored should cooperate in furnishing the records to the State of Occurrence.

5.5.2 Prevent data withholding by the State of Storage

[64] There is only one case where two AIAs could be simultaneously competent: a mid-air collision over the ocean between two aircraft registered in different States. Both States of Registry could claim competence to carry out the investigation. Annex 13 provides no guidance to resolve such a situation and avoid the risk of contradictory findings (one can imagine that both AIAs would cooperate and eventually issue one report each), but that rare situation is not related to the introduction of the QR-FRD system.

[65] AIGP/6-WP/16 Sixth meeting 10-21 May 2021, Proposed amendments to annex 13 and guidance material regarding recovery of automatic deployable flight recorders and protection of transmitted flight recorder data.

One could imagine a scenario where the State of Storage would find an interest, for whatever reason (geopolitical for instance), in withholding the data. It would be in breach of the existing Section 5.14 and the future Section 5.14.2 (if adopted in the proposed terms).

The principle of sovereignty would make it difficult to resolve the situation just by legal means and the most efficient way to prevent that situation would be to lay down a rule obliging the data holder / data center to store at least one backup copy of the FRD in a different State, such as, if possible, the State of Registry or the State of the Operator.

5.5.3 Ensuring timely and efficient transmission of data to the AIA

The very purpose of the QR-FRD project is to ensure "Quick Recovery" of the Flight Recorders Data. Timely transmission of the data to the AIA is therefore of the essence.

Read-out of the flight recorders is always one of the investigation's priority tasks. Section 5.7 of Annex 13 [Ref 8] requires the AIA to "*arrange for the read-out of the flight recorders without delay*" and the *Guidelines for flight recorder read-outs and analysis* (attachment D to Annex 13) insist that "*it is essential that the flight recorders be read out as early as possible after an accident*", as this may reveal problem areas, influence the course of the investigation and even sometimes require immediate safety recommendations.

The project will therefore require immediate access to the data, for which purpose it would be advisable to set up in advance a procedure that would allow the following:

- Quick identification of the data holder: this will of course depend on the choices made for FB4 (off-aircraft storage), but the entity entrusted with storing the data should be identifiable without delay[66] ;
- Quick localization of the decryption key (possibly with the airline);
- Instruction to the data holder to deliver the data at once to the requesting AIA;
- the data holder should not be entitled to refuse the transfer of data on any ground (such as arguing that the requesting AIA is incompetent, or that the data has already been delivered to another entity) so the AIA should identify itself in a way anticipated by the procedure;
- the data holder should not be allowed to deliver the data to anyone except the AIA identifying itself in the manner just described; (the possibility of court orders will be examined separately below at section 5.5.4)
- Third parties that have a legitimate interest in the data (such as judicial authorities or accredited representatives from other AIAs) should not address their requests to the data holder, but to the AIA in charge of the investigation who will copy it to them to the extent necessary and subject to the restrictions of section 5.12 of Annex 13 (protection of personal or sensitive data);
- The data holder should transfer the data directly to the AIA in a secure and crypted way, leaving the AIA in charge of decryption; this may require an amendment to section 3.6.1.4 of ICAO Manual 10054 [Ref 15] which recommends that AIAs receive data "*in a usable (decrypted) format*";

[66] This in itself is an argument in favor of setting up one or a few repositories that AIAs will know beforehand.

- If the data is held by a data center on behalf of one of the involved parties depending on the choices made for FB4), the data center should transfer the data to the AIA directly and not through that involved party.

Such a procedure could be described in ICAO Manual 10054 so that States be encouraged to adopt similar rules at their level.

5.5.4 Regulate judicial authorities' access

Judicial authorities should obtain access to the data through the AIA. The court systems normally do not have investigative authority on foreign territories unless they resort to international mutual legal assistance mechanisms, which considerably slow down their operations: judicial investigators would therefore have an interest in letting the AIA recover the data.

5.5.4.1 Review contents of cooperation agreements between AIAs and judicial authorities

Section 5.4.4 of Annex 13 [Ref 8] recommends that States should ensure cooperation between their AIAs and their judicial authorities and suggests this may be achieved by legislation, protocols, agreements or other arrangements, that should cover issues such as access to evidence, exchange of information, appropriate use of safety information etc.

The implementation of QR-FRD will require AIAs and judicial authorities to review such cooperation agreements.

For instance, such agreements can provide that when two parallel investigations are conducted simultaneously by the AIA and by the judiciary, the judicial investigators will attend the read-out of recorders at the AIA's facilities[67], given that the judiciary is not normally equipped to do the read-out itself, and that a copy of the recordings will be delivered to the judicial investigators[68]. The suppression of the read-out phase will need to be reflected in agreements that refer to it.

With the QR-FDR system, both the AIA and the judicial authorities will receive a copy of the flight data as it is stored by the repository or data center[69]. To guarantee the chain of custody, cooperation agreements could provide for the judicial investigators' presence when the decryption key is being used to make the data readable and immediately obtain a copy.

5.5.4.2 Anticipate potential conflicting requests from judicial authorities of different countries

There are many ways in which judicial authorities from various countries could become involved. As already mentioned, there may be a judicial investigation initiated by the judicial system itself, in the State of Occurrence but also in other States for instance if some of the passengers were their nationals.

[67] Unless the AIA does not have adequate facilities, in which case it will normally use those made available to it by another State.
[68] Subject to the restrictions mentioned at Section 5.12 of Annex 13 for the protection of personal and sensitive data.
[69] Subject to the same restrictions, which will remain applicable.

Courts may also become involved because claims are brought by passengers, by the operator or by their insurers against the aircraft manufacturer or an equipment manufacturer, in cases where the accident might have been caused by a defective product.

Such proceedings can take place in countries totally unrelated to the accident or the investigation (for instance courts of the country where some passengers were domiciled, or those of the headquarters of one of the equipment manufacturers).

In all such cases, parties to the proceedings could ask the courts to issue injunctions against the data repository / data center to deliver copies of the flight data. They would however only obtain crypted data since the data holder should not hold the decryption key. They would therefore need to obtain an injunction against the key holder as well.

Moreover, after 60 days, the recipient of the data should have to delete them if no accident or serious incident has occurred.

This issue is for instance particularly prominent regarding US law as the Cloud Act allows US authorities to request from US companies and subsidiaries the transmission of personal data concerning a US citizen or US habitual resident who is the subject of a criminal prosecution, even if the requested entity has a data center outside of the US[70].

To resist such claims or injunctions, the confidentiality of all or part of the data should be enshrined in legislation or in international law.

At present Annex 13 [Ref 8] allows to regard as confidential only the CVR and AIR records, that are listed at section 5.12; that provision allows to override the confidentiality principle if it is found that the data's disclosure "*outweighs the likely adverse domestic and international impact such action may have on that or any future investigation*".

It would help implement these principles if the CVR and AIR records were clearly identifiable by the data holder even though he only holds crypted data.

5.5.5 Regulate operator's access

As previously mentioned, the operator could be entitled to access part of the FRD, for instance the FDR parameters that are useful to its SMS for the purpose of analyzing flights and incidents. Such data is already often available to the operator through other recordings such as the QAR.

This question falls out of the scope of the present study, which is limited to the QR-FRD process.

It nonetheless raises the issue of management of the decryption key[71]. Rules should be laid down prescribing a procedure for detention of the decryption key (possibly by the airline, thus allowing it to consult the data for SMS purposes) and identifying under which conditions those keys must be delivered to the competent AIA.

[70] Clarifying Lawful Overseas Use of Data Act – H.R. 4943 – 2018.
[71] See envisaged PKI process/structure in QR-FRD Study D3 and D4.

5.5.6 Cases study

The Air Transat Flight TS236 case: the role of QR-FRD systems in case of incident

Unlike the AF447 and the MH370 flight accident cases, the Air Transat TS236[72] flight has landed on an airport. The recorded data were made available "in a timely manner" through a direct access to the physical FDR and CVR recorders. This illustrates situations where data from physical accident recorder would coexist with transmitted data from QR-FRD systems and data from QAR. FDR data used by AIAs, and QAR data used daily by airlines already coexists today. This is the case for all Annex 13 investigations related to serious incidents and accidents followed with a landing.

The Air Transat TS236 accident investigation report[73] indicates: "*A review of aircraft manufacturer and engine manufacturer occurrence databases revealed that since 1994 there have been at least 25 in-flight fuel-leak events. Although some of these events were minor in nature, a number were significant in nature in that they lead to a loss of fuel that resulted in a serious incident, such as an engine fire or a loss of fuel that resulted in a diversion or emergency situation.*".

All these fuel leak events were mandatory reportable events. Related recorded flight data were easily accessible either directly from the aircraft after landing, or by requiring recorded data from the airline FDM program.

It is flight crew and airlines responsibility to report incidents or accidents through mandatory or reporting process. This is a key component of aviation regulatory and safety oversight. It seems important that the implementation of QR-FRD does not make systematic the access to recorded data whenever a trigger has been activated. Such a move could weaken the airline's commitment and responsibility to report. Current regulations do not entitle an AIA to require data from an operator's FDM programme every time an event is detected through this programme.

Indeed, the AIAs entitlement to have access to data remains, whatever happen.

[72] Due to the structural damage and some injuries received during the evacuation the event was an accident per ICAO definition. It could have been « only » an incident.
[73] http://www.gpiaa.gov.pt/

6 Main outcomes summary

The following table summarizes the main different legal issues raised by the new QR-FRD process, as detailed in this report.

FB1: Data Collection / Acquisition and Digitization

• **To ensure AIA's right of access to data** (versus potential data ownership claims by airlines): ownership claims over data already cannot prevent AIA's access and hinder the investigations. No specific amendment needed.
• **To process personal data**:
  ○ Protection of personal data is a fundamental right although the rights of data subjects on their personal data can be limited in case of accident or serious incident
  ○ Technical data may be personal too if it allows to identify crew members' actions. For that reason, and because the GDPR provides for the highest existing level of data protection, the study recommends to apply GDPR data protection standards to all QR-FRD data
• **To ensure data protection and integrity**, the study recommends to:
  ○ Implement encryption techniques coupled with a digital signature in compliance with existing ICAO, GDPR and ISO standards
  ○ Define a key detention policy for airlines

***FB2: Trigger Detection* - Solution #2**

• **To define an efficient policy of trigger detection**, the study recommends to:
  ○ Harmonize the selection of events that will activate the transmission of data. This selection of events can be included in the ICAO Standards.
  ○ Triggers depend on the aircraft type characteristics. The aircraft manufacturer should be responsible for setting them for each specific aircraft type

FB3: Data Transport

• **To ensure the availability of telecommunications networks**, the study recommends to:
  ○ Ensure the availability of dedicated aeronautical frequencies with the ITU
  ○ Ensure the capacity of the infrastructures: mobile and satellite networks
  ○ Moreover, the use of the PIESD is possible according to ICAO Manual 10054
• **To ensure data protection**, the study recommends to address cybersecurity risks through ISO certifications that ensure compliance with GDPR requirements
• **To ensure liability of service providers**: through contractual clauses and certification requirement

FB4: Off-Aircraft Storage
• **To permit data transmission to a data center not originally bound by the GDPR**:

- The GDPR may still apply because of its extraterritorial scope
- A case-by-case examination of the recipient State's data protection legislation will always be required to stipulate appropriate data protection clauses

- **To ensure data protection**, the study recommends to:
  - Ensure data centers' compliance with the GDPR through ISO 27000 certification and contractual clauses
  - Also, ensure protection of data storage infrastructures through ISO 22237-x certifications
  - Provide a data retention and deletion policy through ICAO standards and contractual clauses

- **To identify the most adequate data recipients**:
  - Possible conflict of interests for the existing actors in the field
  - The study recommends to consider a solution that would not rely on one of the actors in the field but on a third party or a dedicated central repository

FB6: Data Recovery

- **To determine the competent AIA**:
  - The QR-FRD does not challenge the fact that the investigation should be conducted by the State of occurrence AIA
  - The study recommends to complete ICAO standards to require the State of storage to transmit the data to the AIA of the State of occurrence

- **To prevent data withholding by the State of storage**, the study recommends to provide a rule requiring the data holder / data center to store at least one backup copy of the QR-FRD in a different State

- **To ensure timely and efficient transmission of data to the AIA**, the study recommends to:
  - Provide a procedure to quickly identify the data holder and the localization of the decryption key
  - Require the data holder to transmit encrypted data only to the competent AIA
  - Require that third parties legitimately interested in the flight data address their request to the competent AIA and not to the data holder
  - Complete ICAO Manual 10054 to recommend the implementation of efficient procedures

- **To regulate judicial authorities' access**, the study recommends to**:**
  - Review cooperation agreements between AIAs and judicial authorities
  - Strengthen the confidentiality of data in ICAO standards to address data requests from foreign judicial authorities
  - Enable the data holder to quickly identify encrypted CVR and AIR data

- end of document -

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union